Texas Interpreters Fellowship

5811 Woodcraft, San Antonio, TX 78218
Phone (210) 666-2123 / Fax (210) 661-7627
Text/MMS (210) 666-8120
www.tifsa.com / tifsa@tifsa.com

POLICY FOR PASSWORD STANDARD

Last updated 14 February 2021

INTRODUCTION

Texas Interpreters Fellowship (TIF) recognizes it's affirmative and continuing obligation to protect the confidentiality, maintain the integrity, and ensure the availability of information about and used by TIF staff, interpreters, contractors, vendors, and customers and to provide administrative, technical and physical safeguards to protect TIF information assets.

Passwords are an important aspect of computer security. They are the front line of protection for user accounts. Passwords can preserve the confidentiality of password-protected data and are the sole property of account holders. As such, all Texas Interpreters Fellowship (TIF) staff, interpreters, contractors, vendors, and any person authorized to access TIF confidential information and systems, are responsible for taking the appropriate steps, as outlined below, to select and secure their passwords.

The purpose of this Policy is to communicate the composition of strong passwords, the protection of those passwords, and the frequency of change.

POLICY SCOPE

This Policy for Information Security and Privacy applies to:

1. Staff, interpreters, contractors, sub-contractors, vendors, consultants, and any other authorized persons having access to confidential information.
2. computing devices and/or electronic storage media with access to TIF resources or that stores confidential information from TIF.

DEFINITIONS

Authorize Purpose – means the specific authorized purpose or purposes for which a person needs to have access to Confidential Information in order to fulfill their obligations to TIF, or any other purpose expressly authorized by TIF.

Authorized User – A Person:

1. Who is authorized to create, receive, maintain, have access to, process, vie, handle, examine, interpret, or analyze Confidential Information;
2. For whom TIF warrants and represents has a demonstrable need to create, receive, maintain, use, disclose or have access to Confidential Information;
3. Who has agreed in writing to be bound by the disclosure and use limitations pertaining to the Confidential Information as required by this policy.

Confidential Information – Information which concerns or relates to Protected Health Information (PHI), Personal Identifiable Information (PII), HIPAA regulated information, trade secret, know-how, invention, software program, application, documentation, schematic, procedure, contract, information, knowledge, data, process, technique, design, drawing, program, formula or test data, work in progress, marketing, financial, sales, supplier, customer, employee, investor, or business information, or other information of commercial value, whether in oral, written, graphic or electronic form. Confidential information also includes, but not limited to, any information as defined by customers, local, State and Federal contracts, rules and regulations to be confidential.

Partially funded through

Texas Health and Human Services (HHS) Office of Deaf and Hard of Hearing Services (DHHS)

Policy for Password Standard

Electronic Computing Device – Include, but not limited to, desktop computers, laptop computers, PDAs, tablet PCs, and smart phones.

Electronic Devices – Include, but not limited to, Electronic Computing Devices and Electronic Storage Media.

Electronic Storage Media – Include, but not limited to, CD-ROMs, DVD-ROMs, external hard drives, zip drives, floppy disks, reel and cassette format magnetic tapes, flash-memory cards, magnetic cards, and USB flash drives (a.k.a. Memory sticks, Thumb or Jump drives).

Information – Any communication or representation of knowledge such as facts, data, or opinions in any medium or form; including oral, written, graphic, electronic form, numerical, cartographic, narrative, or audiovisual forms.

Protected Health Information (PHI) – "Individually identifiable health information" held or transmitted by a covered entity or its business associate, in any form or media, whether electronic, paper, or oral. “Individually identifiable health information” is information, including demographic data, that relates to:

- the individual’s past, present or future physical or mental health or condition,
- the provision of health care to the individual, or
- the past, present, or future payment for the provision of health care to the individual that identifies the individual or for which there is a reasonable basis to believe it can be used to identify the individual. Individually identifiable health information includes many common identifiers (e.g., name, address, birth date, Social Security Number).

The HIPAA Privacy Rule excludes from protected health information employment records that a covered entity maintains in its capacity as an employer and education and certain other records subject to, or defined in, the Family Educational Rights and Privacy Act, 20 U.S.C. §1232g. (Defined in the HIPAA Privacy Rule).

Personally Identifiable Information (PII) – Information which can be used to distinguish or trace an individual's identity, such as their name, social security number, biometric records, etc. alone, or when combined with other personal or identifying information which is linked or linkable to a specific individual, such as date and place of birth, mother’s maiden name, etc.

POLICY ROLES AND RESPONSIBILITIES

Owner, Staff, Interpreters, Contractors, Sub-Contractors, Vendors

Owner, Staff, interpreters, contractors, sub-contracts, vendors, and any other individuals whom may have or do have access to confidential information (Authorized User(s)), for any authorized purpose(s), must ensure that they comply with TIF's policies and procedures to ensure that the Confidential Information is kept safe and secure. In addition to ensuring compliance, they must also report any suspected or actual incidents that can or has resulted in privacy and security violations.

This standard applies to all authorized users who have or are responsible for an account or any form of access that supports or requires a password on any electronic device, has access to TIFs online services or network, or stores any confidential information.

PASSWORD COMPOSITION

Passwords are used for various purposes. Some of the more common uses include: user level accounts, email accounts, screen saver protection, and local router logins.

Passwords shall at least adhere to the following complexity guidelines:

- Be case sensitive
- Be at least eight characters in length
- Contain three of the following four character types:
    - Uppercase English characters (A through Z)
    - Lowercase English characters (a through z)
    - Numbers (0 through 9)

- Special characters (` ~ ! @ # $ % ^ & * ( ) _ + - = { } | [ ] \ : " ; ' < > ? , . /)

- Contain no spaces
- Include no part of a person's full name
- Contain no non-English language characters
- Not match any of a person's previous passwords

To the extent that password complexity is supported by respective devices and/or systems, passwords should also:

- Not contain personal information such as user name or CSULB ID number
- Not contain a complete dictionary word from English or another language
- Be significantly different from previous passwords
- Not be incremental with every password change (Example: Password 1, Password 2, Password 3...)
- Be difficult to crack, but easy to remember (Example: make up a sentence, and then use the first letter of each word or sound, adding a couple of digits or symbols and uppercase letters. For instance, "Tennis later anyone??" becomes the password: "10sL8rne1??" or "I really love 8 hot fudge sundaes best," becomes "irL8htfsB!"
- Not have more than two characters repeated consecutively
- Not use adjacent keyboard characters (Example: asdfghjkl:, qwertyuiop, 1234567890)

PASSWORD PROTECTION

Your password is to be treated as confidential information. To protect your confidential information, you should take the following measures:

- Do not use the same password for TIF accounts as for your personal accounts, where possible.
- Do not reveal a password over the phone to ANYONE.
- Do not reveal a password in an email message.
- Do not talk about your password in front of others.
- Do not hint at the format of your password (e.g., "my dogs name").
- Do not reveal a password on questionnaires or forms.
- Do not reveal a password to Authorized Users while on vacation.
- Do not reveal a password to Unauthorized Users.
- Do not write passwords down and store them anywhere that is not secure.
- Do not store passwords in a file on ANY computer systems without encryption.
- Do not use the "Remember Password" feature of applications or web browsers.

PASSWORD CHANGE FREQUENCY

Passwords should be changed at least every 90 days but no password should remain unchanged for more than a year.

Check with TIF to find out if any client specific contracts require password changes to be made in a specific time other than above.

PERIODIC REVIEW

TIF's owner and/or Information Security Officer shall conduct an annual and, as needed, periodic review of this policy for Information Security and Privacy to ensure that it remains appropriate and relevant.

Policy for Password Standard

INFORMATION AND ASSISTANCE

Texas Interpreters Fellowship will make available this and all applicable policies on their website at https://www.tifsa.com/_tos.html.

Direct any questions, comments, suggestions, or requests for further information to the Owner of Texas Interpreters Fellowship by email at tifsa@tifsa.com or by mail at Attention: Owner, Texas Interpreters Fellowship, 5811 Woodcraft, San Antonio, Texas, 78218.