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 PERSONALLY OWNED ELECTRONIC COMPUTING DEVICE AND STORAGE MEDIA 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.

This purpose of this policy is to ensure that all personally owned electronic computing devices and/or electronic storage media are configured and used appropriately when accessing Texas Interpreters Fellowship resources.

Policy Scope

This Policy applies to:

- Staff, interpreters, contractors, sub-contractors, vendors, and any other authorized users which access to confidential information; and
- 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;For whom TIF warrants and represents has a demonstrable need to create, receive, maintain, use, disclose or have access to Confidential Information;
2. 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), HIPPA 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.

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.

Partially funded through

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

Policy for Personally Owned Electronic Computing Device and Storage Media Standard

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 (aka Memory sticks, Thumb or Jump drives).

Encryption – The process of altering electronic information using a code or mathematical algorithm so as to be unintelligible to unauthorized users. Encryption software and assistance can be obtained through Information Technology Services.

Incident – The act of violating and explicit or implied security policy. Incident can also include any situation that can or does lead to the loss or release of confidential information to unauthorized individuals.

These include but are not limited to:

1. The loss of a mobile device that is used to access or receive confidential information.;
2. Attempts (either failed or successful) to gain unauthorized access to a system or its data;
3. Unwanted disruption or denial of services;
4. The unauthorized use of a system for the processing or storage of data; and
5. Changes to system hardware, firmware, or software characteristic without the owner's knowledge, instruction, or consent.

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.

Malware – Short for "malicious software," malware refers to software programs designed to damage or perform other unwanted actions on a computer system. Common examples of malware include viruses, worms, trojan horses, and spyware.

Operating System – Also known as an "OS," this is the software that communicates with computer hardware on the most basic level. Without an operating system, no software programs can run. The OS is what allocates memory, processes tasks, accesses disks and peripherals, and serves as the user interface. Examples of operating systems include Microsoft Windows, Apple Macintosh (Mac), and Linux.

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.

Software – Computer software is a general term that describes computer programs. Related terms such as software programs, applications, scripts, and instruction sets all fall under the category of computer software. Therefore, installing new programs or applications on your computer is synonymous with installing new software on your computer. Examples of software include Microsoft Word, Microsoft Excel, Adobe Acrobat, etc.

Policy for Personally Owned Electronic Computing Device and Storage Media Standard

POLICY ROLES AND RESPONSIBILITIES

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

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.

STORAGE OF CONFIDENTIAL/INTERNAL USE CONTENT ON COMPUTING DEVICES/ELECTRONIC STORAGE MEDIA

All confidential information that is used and collected by Texas Interpreters Fellowship must be stored on TIFs owned, or authorized, and secured databases or file servers. This information may be accessed by authorized users only from electronic devices authorized by TIF and meet the policy requirements established by TIF.

For information accessed, used, and stored by interpreters, contractors, sub-contractors, or any other person providing services to TIF and authorized access to TIF's confidential information will ensure that their electronic devices meet or exceed the requirements of this policy.

No authorized user will store TIF's confidential information on any electronic device that does not meet the requirements of this policy and that is not authorized by TIF.

No confidential information can be stored on free cloud services.

ACCESSING CONFIDENTIAL/INTERNAL USE CONTENT WITH A COMPUTING DEVICE

All Authorized Users personally owned electronic devices accessing TIF's resources shall meet the following minimum standards:

- Maintain a currently patched/updated operating system. Patches and updates are available from the respective operating system vendor and should be applies, either automatically or manually, as soon as possible after they are released.
- Current anti-virus software installed, activated, and regularly updated. Software should be from a recognized vendor such as Avast, McAfee, Microsoft, Sophos, Symantec, etc. All electronic devices must have anti-virus software installed.
- Periodically scan electronic computing devices to detect malware.
- Use strong passwords (refer to TIF's Password Standard)
- Regularly update all software with security patches.
- Delete cookies, history, and temporary files upon exiting the internet browser software.
- Ensure that any electronic device that will no longer be used to store or access Confidential Information is properly erased/destroyed to ensure that no Confidential Information can be accessed.
- All electronic devices must also meet any TIF client requirements.

Use of Email to Transfer Confidential Information

Confidential information may only be transferred by email to those with an established business need-to-know and are either TIF staff or someone who has signed a confidentiality agreement. Email with confidential information must not be sent over a public network unless password protected or encrypted. All email transmissions of confidential information must contain the following statement:

> "The content of this message is confidential. If you have received it by mistake, please inform us by an email reply and then delete the message. It is forbidden to copy, forward, or in any way reveal the contents of this message to anyone. The integrity and security of this email cannot be guaranteed over the Internet. Therefore, the sender will

> not be held liable for any damage caused by the message. Unauthorized interception of this message may be in violation of the Electronic Communications Privacy Act, 18 U.S.C. §2510 et seq."

TIF Internal Use information may only be transferred by email to TIF staff and those individuals with a business need-to-know. Email may be sent or over an approved public network to persons with a business need-to-know.

PERIODIC REVIEW

TIF shall conduct an annual and, as needed, periodic review of this policy to ensure that it remains appropriate and relevant.

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.