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 INFORMATION SECURITY AND PRIVACY

Last updated 14 February 2021

INTRODUCTION

Texas Interpreters Fellowship (TIF) recognizes its affirmative and continuing obligation to protect the confidentiality, maintain 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.

Texas Interpreters Fellowship Policy for Information Security and Privacy provides the framework for assisting TIF with meeting its responsibilities to:

1. Safeguard personal and confidential information of TIF staff, interpreters, contractors, and customers and other TIF sensitive data regardless of format or medium;
2. Protect against anticipated threats or hazards to the physical security or integrity of TIF information assets;
3. Protect the privacy of TIF staff, interpreters, contractors, and customers by preventing non-permitted disclosure of personal and confidential information; and
4. Ensure company compliance with federal and state law, regulations, TIF policies, procedures, and standards regarding information security and privacy.

POLICY SCOPE

This Policy for Information Security and Privacy applies to:

1. Information that is acquired, transmitted, processed, transferred, and/or maintained by TIF;
2. All data systems and equipment including desktops, mobile devices, cloud services, and other ancillary systems and equipment as well as data residing on these systems and equipment;
3. Home/personal electronic devices of TIF staff, interpreters, contractors, sub-contractors, vendors, and any other authorized users which access to confidential information; and
4. Staff, interpreters, contractors, sub-contractors, vendors, consultants, and any other authorized persons having access to confidential information.

Texas Interpreters Fellowship shall do the following:

1. Report security and privacy incidents. If any suspected or actual loss of Confidential Information TIF shall ensure to report the incident to anyone who is determined to possibly be or is affected by the incident and to notify the proper authorities;
2. Coordinate a company-wide response to security vulnerabilities, threats, and incidents; and
3. Facilitate company-wide sharing of information regarding security vulnerabilities, threats, and incidents; and
4. Provide (or augment existing) analysis capabilities and/or forensic services with respect to security vulnerabilities, threats, and incidents, particularly if TIF does not have the capabilities.
5. TIF shall establish and maintain security and privacy incident response capabilities, or ensure that incident capabilities are performed on their behalf.

Partially funded through

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

Policy for Information Security and Privacy

DEFINITIONS

Authorize Purpose – means the specific authorized purpose or purposes for which a person needs to have access to Confidential Information 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 is not limited to, any information as defined by customers, local, State ,and Federal contracts, rules, and regulations to be confidential.

Incident – The act of violating an 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 characteristics 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.

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 that is linked or linkable to a specific individual, such as date and place of birth, mother’s maiden name, etc.

Policy for Information Security and Privacy

POLICY ROLES AND RESPONSIBILITIES

Owner

The responsibilities of the Owner of Texas Interpreters Fellowship include but are not limited to the following:

1. Establish, implement, and enforce a Company-wide framework to facilitate the safety and security of all of the company's confidential information.
2. Ensure the Company-wide implementation of applicable Federal, State, local, and Client contractual required policies and procedures related to the security and safety of all Confidential Information.
3. Manage the resources that support the company's operations.

Information Security Officer

Information and Security Officer (ISO) is an appropriate administrator designated by the owner, or is the owner, of TIF and delegated responsibility for developing policies, procedures, and standards regarding the acquisition, transmission, processing, maintenance, safeguarding, release, and disposal of personal and confidential information and other TIF sensitive data; developing training and informational materials; and assessing and ensuring the TIF's compliance with applicable laws, regulations, and TIF policies, procedures, and standards regarding information retention, security, and privacy.

Staff, Interpreters, Contractors, Sub-Contractors, Vendors

Staff, interpreters, contractors, sub-contracts, vendors, and any other individuals who 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 have resulted in privacy and security violations.

Authorized Users must, in writing, confirm that they have been notified of this policy (see Attachment A) and that they will comply with all parts of this policy and any additional policies and procedures that TIF establish to ensure that Confidential Information is kept safe and secure. In addition ,they must also, in writing, confirm compliance with any of TIF's client's contractual requirements in regards to keeping Confidential Information safe and secure.

TRAINING

Texas Interpreters Fellowship will ensure that all authorized users covered by this policy receive training within 30 days upon being hired and annual training covering keeping Confidential Information safe and secure.

Authorized users that may have or do have access to information covered by HIPAA must receive HIPAA training before having access to covered HIPAA Confidential Information. Interpreters must also attend annual HIPAA refresher training. Authorized users must provide proof of this training to TIF.

TIF will ensure that the training provided to covered individuals is accurate and complete. If the training is not accurate and complete then TIF will ensure the training is corrected and brought into compliance with this policy and that all covered individuals retake the corrected training within 30 days.

TIF will maintain records that document when the training is completed by each covered individual and ensure that annual training is completed by each covered individual. Any individual that does not complete the training required by this policy will not have access to any Confidential Information.

REPORTING OF AN INCIDENT

Whenever it is suspected or there is an actual situation that can result in the exposure and/or loss of confidential information the authorized user must notify, if applicable, the proper authorities (i.e. the police) and TIF immediately. Failure to promptly notify TIF will result in the immediate denial of access to Confidential Information and suspension until a full review of the situation can be determined and appropriate action taken.

Examples of reportable incidents include but are not limited to:

- Theft or loss of phone, laptop, or portable device, or any type of written form that contains confidential information

- Illegal access and use of phone, laptop, computer, or portable device (i.e. hacking of computer, electronic device exposed to a virus)
- Theft or illegal access to any confidential information or areas containing confidential information
- Purposely or accidentally sharing confidential information with anyone not authorized by TIF

Upon notifying TIF, the person reporting the incident must provide, in writing, a complete and accurate statement that details the incident, actions that are taken, and what confidential information is involved, if known. This written statement must include to whom they notified of the situation and if known any actions that were taken by them and their contact information. This written statement must be submitted to TIF immediately so that it can be used to help determine what was lost and what actions to take.

RESPONDING TO A REPORTED INCIDENT

Upon notification of an incident, TIF will immediately begin to take action to mitigate the situation. TIF will begin a detailed log that will document every detail and action taken until the incident is resolved.

TIF will notify all clients and persons who are possibly or actually affected by the incident within the 1st hour of notification, if possible, and know. TIF will fully cooperate with all affected clients, Individuals, and investigating authorities.

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.

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.

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

Attachment A: Authorized Users Confirmation and Agreement Form

Texas Interpreters Fellowship's ("TIF") Policy for Information Security and Privacy ("Policy") established the permitted and required uses and disclosures of Confidential Information by Authorized Users.

Authorized Users are subject to the Policy and any contractual requirements established by TIF's clients. Authorized Users acknowledges, understands, and agrees to be bound by the identical terms and conditions applicable to the Authorized User under this Policy, incorporated by reference in this Agreement, with respect to Confidential Information.

Authorized Users assures TIF that any Event as defined by the Policy that the Authorized User discovered will be reported to TIF in the time, manner, and content required by this Policy.

If TIF knows or should have known in the exercise of reasonable diligence of a pattern of activity or practice by Authorized User that constitutes a material breach or violation of the Policy or the Authorized User's obligations TIF will:

1. Take reasonable steps to cure the violation or end the violation, as applicable;
2. If the steps are unsuccessful, terminate the contract, employment, or arrangement with TIF, if feasible;
3. Notify Clients and, if applicable, proper authorities upon reasonable discovery of the pattern of activity or practices of Authorized User that constituents a material breach or violation of the Policy and keep all notified clients and authorities reasonably and regularly informed about steps TIF is taking to cure or end the violation or terminate Authorized User contracts, employment or arrangement.

This Confirmation Form is executed by the parties in their capacities indicated below.

Texas Interpreters Fellowship	**Authorized User**
Signature:	Signature:
Name: Kathi **Ayres**	Name:
Title: **Owner**	Title:
	Date:

Partially funded through

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