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

ELECTRONIC MEDIA SANITIZATION PROCESS

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.

The purpose of this Policy is to guide Authorized Users and information technology coordinators through the use of TIF's standardized tool and processes to securely sanitize electronic devices that are being:

- Disposed of (e.g drive is too small, or no longer needed);
- Reassigned to other individuals; or
- Recycled or reused.

This is necessary to reduce the possibility of inappropriate exposure of data and unauthorized use. To protect the confidentiality of information authorized users must ensure that electronic data in their possession is secure at all times.

When electronic computing devices and/or electronic storage media are transferred, recycled, or removed from service, all electronic data must be properly sanitized before the release of custody. The sanitization process ensures that recovery of information is not possible and that TIFs information security objectives are not compromised. Several methods can be used to sanitize media; however, the two major types of sanitization are clearing and destroying.

Clearing

Clearing information is a level of media sanitization that protects the confidentiality of information against a robust keyboard attack. Simple deletion of items does not suffice for clearing. Clearing must not allow information to be retrieved by data, disk, or file recovery utilities and must be resistant to keystroke recovery attempts executed from standard input devices and data scavenging tools.

Partially funded through

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

Electronic Media Sanitization Process

Overwriting is an acceptable method for clearing media. The security goal of overwriting is to replace written data with random data

There are several overwriting software products to overwrite storage space on media. Overwriting cannot be used for media that are damaged or not rewritable. In such cases, electronic media should be destroyed.

Destroying

When electronic media is inoperable and cannot be cleared, the electronic media must be physically destroyed. While physical destruction can be accomplished using a variety of methods, the authorized user must ensure to use a service that can provide certification of the electronic device and that any confidential information is secure and irretrievable. For media that can be run through a shredder, the authorized user must fill out and submit an Electronic Device Sanitization Certification form.

POLICY SCOPE

This Policy applies to:

- Staff, interpreters, contractors, sub-contractors, vendors, and any other authorized users which access confidential information; and
- computing devices and/or electronic storage media with access to TIF resources or that stores confidential information from TIF.

DEFINITIONS

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 of 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 is 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 is not limited to, desktop computers, laptop computers, PDAs, tablet PCs, and smartphones.

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 (aka 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 that 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

Electronic Media Sanitization Process

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.

TRANSFERRING, SURVEYING, OR DESTROYING ELECTRONIC DEVICES AND MEDIA

When electronic computing devices or electronic storage media are to be transferred or surveyed, authorized users must ensure the following steps are completed:

1. All electronic computing devices or electronic storage media must be overwritten using TIF-approved and validated overwriting technologies/methods/tools without exception.
2. Only instances involving an inoperable hard drive that cannot be cleared will require its' removal from the electronic computing device to ensure proper destruction. Inoperable electronic computing devices and/or electronic storage media must be isolated and secured until properly destroyed. These devices will be destroyed using a service that can provide written certification of the electronic device's destruction and safety of confidential information. A copy of the written certification must be provided to TIF.
3. Authorized Users must complete and sign an Electronic Device Sanitization Certification form (see attachment A) for the item(s) to be transferred, surveyed, or shredded.
4. The Electronic Device Sanitization Certification must be submitted to TIF.
5. Upon approval from TIF, the item(s), if being transferred, may then be transferred.

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.

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: Electronic Device Sanitization Certification

I certify that the following electronic computing devices and/or electronic media have been properly cleared and/or destroyed as per Texas Interpreters Fellowship's Electronic Media Sanitization Process process.

Make

Model

Serial Number

Manufacture

Manufacture Date

□ **Data has been overwritten.**

□ **The hard drive has been removed for destruction/degaussing.**

□ **Not Applicable. No data stored on the electronic computing devic**

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

Partially funded through

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