WORKFORCE SOLUTIONS FOR TARRANT COUNTY
A proud partner of the AmericanJobCenter network

Data Handling & Incident Reporting Guide

Terminology

The state and federal policies, standards, and laws that govern Workforce Solutions for Tarrant County's (WSTC's) business activities use a variety of terms to describe information that must be protected (see TWC's Cybersecurity Awareness Training for a more detailed breakdown). Personally Identifiable Information (PII) and Sensitive Personal Information (SPI) are defined below for clarity.

In addition to PII and SPI, the data handling guidelines in this document also apply to other sensitive information that may not identify individuals but still must be protected. Examples of "other sensitive information" include WSTC's internal IP addresses, equipment serial numbers, and investigation notes.

Any reference to PII throughout this document and the IT Policies and Procedures Manual should be interpreted to include PII, SPI, and other sensitive information. If you have any questions or concerns regarding data handling procedures, ask your supervisor or email privacy@workforcesolutions.net.

Personally Identifiable Information (PII)

PII is any information that identifies an individual, directly or indirectly. Due to the broad nature of this definition, some PII may be publicly available and not designated as sensitive or confidential under federal or state law. **However, WSTC Users are still contractually and ethically obligated to handle this information with caution.**

Examples of Publicly Available PII:

- Names, addresses, telephone numbers, and places of work on a business card
- Names, addresses, and telephone numbers in a public phone directory
- List of agency employee names

Sensitive Personal Information (SPI)

Sensitive Personal Information is a subset of Personally Identifiable Information, which if lost, compromised, or disclosed without authorization, could result in substantial harm to an individual. Therefore, **Sensitive Personal Information** requires stricter handling guidelines because of the increased risk to an individual if the data is compromised.

Some categories of PII are considered **SPI** as stand-alone data elements. **The most common example is a Social Security Number (SSN).** Other categories of PII are considered **SPI** when used in combination with other identifying information, such as an individual's first initial and last name – J. Smith. **For further information regarding SPI, see TWC's Sensitive Personal Information Training.**

Workforce Solutions for Tarrant County
Data Handling & Incident Reporting Guide

What is Personally Identifiable Information (PII)? **PII includes:** Name, email, address, phone number	
Sensitive Personal Information (SPI) includes:	
If Stand-Alone:	**If paired with another identifier:**
• Social Security Number	• Citizenship or immigration status
• Driver's License Number	• Employee or personnel records
• Alien verification number	• Account passwords
• Financial account number	• Last 4 digits of SSN
• Passport number	• Date of birth
• Biometric identifiers (fingerprint, voice print)	• Criminal History
	• Mother's maiden name
	• Educational information
	• Medical information, including disability-related information

When approaching security of PII, keep three guiding principles in mind:

1) Protect other people's PII the way you would want your PII protected.
2) Context matters. A list of public meeting attendees is not SPI, but a list of program participants is SPI.
3) When in doubt, always protect PII.

Physical Security

- All WSTC-managed facilities must be security guarded or other perimeter security controls.
- All WSTC-managed facilities must track visitor/guest access with a sign in/out log.
- Visitors at WSTC-managed facility must wear a WSTC-issued visitor badge.
- All guests visiting non-public areas must be escorted at all times.
- At least 2 barriers of protection for PII (see page 3) must be maintained at all facilities used by WSTC Users.
- **Any equipment used to access PII, such as access badges, keys, or telecommunications devices used for authentication purposes, must be protected the same as PII and secured using the two-barrier minimum standard.**
- When possible, shred documents that include PII and other sensitive information after use.
- Store documents containing PII in a locked location when not actively in use.
- Never leave documents that include PII and other sensitive information in plain view.

PII BARRIER EXPECTATIONS (Minimum 2 required)			
Area	**During Hours of Operation**	**After Hours**	**Additional Barrier**
Restricted*	Staff serves as an escort to all visitors and monitors visitor activity	Locked building, security guard	Out of plain sight
Secured	Authorized staff only	Locked building, security guard	Locked; access control
Public	Staff monitored	Locked building, security guard	Locked; staff distributes documents with PII to customers

*As identified by signage such as "Employees Only"

Electronic Security

- Only WSTC-approved equipment/systems may be used to send, receive, process, access, and store PII and other sensitive information.
- Do not share passwords or any data or equipment used for authentication and identification purposes.
- Lock or log off of computers when leaving them unattended, no matter for how short a time.
- Files containing PII may be stored in shared network access drives ("shared drives") only if access is restricted to those with a need to know through permission settings or passwords.
- PII downloaded to or maintained on mobile/portable devices must be encrypted.
- Encryption software must be FIPS 140-2 compliant and meet NIST-validated cryptographic standards. ***Ask the IT Department if you're not sure if your encryption method meets this standard.***

Proximity Awareness

When PII is handled, processed, transmitted, and/or stored, **users** must limit the potential for unauthorized disclosure. **Users** in all areas, whether in restricted or unrestricted areas, should protect against "shoulder surfing," eavesdropping, or overhearing by anyone without a need to know the PII.

Workforce Solutions for Tarrant County
Data Handling & Incident Reporting Guide

Emailing

- Email PII only to authorized individuals with a legitimate need to access said information.
- Avoid unnecessary forwarding and/or copying of emailed PII.
- **Sensitive Personal Information, such as Social Security Numbers and Driver's Licenses, must not be emailed unless management determines that there is a strong business case for including that information and there is no reasonable alternative (e.g. TWIST ID).**
- PII and other sensitive information transmitted via email must be sent in an encrypted attachment or through e-mail software that encrypts the entire message and its attachments. Attachment passwords must be a minimum 8 characters, contain a mix of capital letters, lower case letters, numbers, and special characters and be provided to the recipient through a separate medium (e.g. in person, separate email thread, phone call).
- WSTC Users with workforcesolutions.net email addresses may securely send PII to other workforcesolutions.net email addresses as encryption is handled through IT-managed configuration of the email system. E-mails sent outside the WSTC domain must be manually encrypted by placing the 2 words *Encrypt This* in the subject line.
- Do not send PII in the subject line or body of an e-mail in clear text (not encrypted).
- Blind carbon copy (BCC) or WSTC-approved software must be used for emails containing multiple customer recipients.

Printing, Faxing and Scanning

- Do not print to an unattended printer unless physical access controls, such as private print, are used to prevent unauthorized access.
- Avoid unnecessary duplication of PII and other sensitive information.
- Minimize the time PII is left on printers and faxes.
- All faxes must be sent with a cover page including the recipient name and fax number and the sender name and fax number as well as a confidentiality statement at the bottom of the page.
- When faxing PII, the recipient must be alerted prior to sending.
- Machines programmed to receive faxes must be in secured or restricted areas.
- Fax transmission errors for faxes containing PII should be reported as a possible security/privacy incident.

Mailing

- Mailed PII materials must be enclosed in an opaque container to hide identifying information other than name and address.
- Use the U.S. Postal Service's first-class mail, priority mail, or an accountable commercial delivery service. Package tracking services must be used for mailed PII.
- Double-wrapping or double-boxing of mailed PII is recommended.
- Electronic devices and/or media must be encrypted prior to mailing.

Workforce Solutions for Tarrant County
Data Handling & Incident Reporting Guide

Phone Transmission

- Do not leave PII on voicemail and do not request that PII be left on your voicemail.
- Do not send PII via text/SMS message or instant message and do not request PII via IM or text.
- Discuss PII only in a secure location where information cannot be overheard by unauthorized individuals.
- Do not release PII over the phone except to the customer whose data it is, and then only after the customer provides enough information to establish their identity.

Traveling, Transporting, and Storage in Vehicles

- Transported PII must remain with the individual and kept from unauthorized disclosure.
- Only authorized WSTC Users designated by management may transport PII.
- All PII removed from an office must be documented. A transmittal form that incorporates a sign-out/sign-in protocol or other chain of custody logging method must be created and implemented.
- Laptops, mobile devices, portable storage devices, and files containing PII must not be left in vehicles unattended for significant periods of time. If PII must be left for a short period of time, the PII must be placed in the trunk, if available, or out of plain sight. The vehicle must be locked.
- Transported PII must be removed and secured upon arrival at the intended destination.

Disposal/Destruction

- PII and other sensitive information, in electronic and paper form, must be destroyed in accordance with TWC guidelines at the end of WSTC's retention policy period.
- Printed PII must be destroyed using a cross-cut shredder or transferred to a WSTC-approved shred vendor for final disposal.
- Shredded material or material awaiting transfer to a shred vendor must be stored in an opaque container in a secure or restricted location (e.g. locked shred bin) in preparation for permanent destruction.
- WSTC-approved shred/disposal vendors must be used.
- Do not use recycle bins for disposing of PII and other sensitive information.
    - Computer drives, mobile devices, and other electronic storage devices containing PII must be wiped utilizing NIST 800-88 approved methods prior to being reissued or when they are designated for disposal. ***Ask the IT Department if you're not sure if your disposal/destruction method meets this standard.***

Telecommuters

- PII, in either paper or electronic format, must not be taken home or to any non-WSTC approved worksite, unless required to conduct WSTC business and appropriately secured (e.g. locked home office, file cabinet, drawer, or hotel safe).
- **Use of a personally-owned computer to connect to WSTC networks must be preauthorized.**
- Personally-owned computers or email accounts must not be used to download, save, store, or host PII.
- Personally-owned printers must not be used to print, copy, scan, or fax PII.
- Screen shots or other personal storage of PII is forbidden, including Dropbox, Google Docs, and Evernote.
- **VPN access is only authorized on IT-approved equipment.**
- It is the responsibility of users with telecommuting privileges to ensure that unauthorized users are not allowed access to WSTC systems, equipment, applications, or accounts.

Suspicious Emails

WSTC Users should handle unsolicited or suspicious emails with extreme caution. If a suspicious email is received, users must take the following action:

1. **Do NOT click on any links;**
2. **Do NOT open any attachments;**
3. **Do NOT respond to the email;**
4. **Do NOT forward the email to anyone;**
5. **Take a screen shot of the suspicious email, including the To, From, Subject, and Body of the email;**
6. **Send the SCREEN SHOT ONLY to cso@workforcesolutions.net for review; and**
7. **Highlight the email in your message list; then press the Shift and Delete keys simultaneously. This action will permanently delete the email from your account.**

Security/Privacy Incidents

WSTC defines a privacy incident as the suspected or confirmed threat of unauthorized access, use, acquisition, disclosure, modification, or destruction of WSTC's Information Resources and/or PII and other sensitive information. Examples of security/privacy incidents include:

- Computer system and/or network intrusion;
- Computer virus or other malware detection;
- Suspected or actual breaches, compromises, or other unauthorized access to WSTC systems, equipment, applications, or accounts;
- Unauthorized changes to computers or software;

- Loss or theft of WSTC-issued computer equipment, mobile devices, removable media, or other data storage devices and media;
- Loss or theft of any personally-owned mobile device **or other equipment** used for business **purposes**;
- Loss or theft of personnel or customer files/paperwork; or
- Inappropriate or improper usage of WSTC Information Resources and/or PII and other sensitive information.

All WSTC Users are required to perform the following related to a security/privacy incident:

- At the time of discovery, secure affected equipment, systems, and/or data from further compromise.
- Notify your supervisor/manager AND the Chief Security Officer (817-413-4499 **or through Incident Form on the IT Hub**) immediately upon incident discovery.
- Cooperate with the Chief Security Officer and other designated IT security staff by completing an Incident Report and maintaining records about the incident.
- Do not engage in gossip regarding an ongoing incident investigation. Discuss the incident only with IT security staff and those with a legitimate business need to know.
- Do not forward compromised information to anyone. If compromised information is needed as part of an investigation, IT security staff will provide instructions regarding transfer procedures.

Managers & Supervisors are required to perform the following related to a security/privacy incident:

- Ensure **users** timely report incidents to the board Chief Security Officer (817-413-4499).
- Ensure **users** timely complete incident documentation.
- Assist IT security staff as needed with any incident investigation and fact-finding activities.