

Linking Jobseekers and Employers

Employee Information Coversheet

Name:					
Position:		Office:		Workstatio	n Name:
Date:		Manager:			
New User	Access Cha	nge / Transfer	🛛 Annu	al Update	Termination

User Access: (Check all that apply)

	Network Access (Windows)
	Dutlook E-mail
	Company Shared Drive
L F	RACF Mainframe Access
דם	TWIST
ד 🗆	TIERS
	Nork In Texas
	CCS Workflow
	New Phone Extension
If No, lis	t current ext.
	ntern
	WFSHOT Intranet
	Dther

Department Assignment

Board
BSU
Career Center
CCS
Choices / Snap
CIS
Veteran Services
WIOA
WFC Management
Other

Management Approval
Signature: ______

Date: _____

NOTE:

Please be sure to complete ALL forms for access requests. New Employee Packet for new hires can be found on the shared drive. Attach appropriate change form for access change requests.

For IT Staff Only: Request received on:	Complete packet received on:
Request completed on:	Signature:

HEART OF TEXAS WORKFORCE BOARD and Workforce Solutions Heart of Texas CENTERS

Acceptable Use Policy

EMPLOYEE COPY

YOU MUST READ THIS POLICY AND KEEP FOR YOUR RECORDS

This policy defines the acceptable use of computer software, hardware, and network resources for the Heart of Texas Workforce Board (the Workforce Board), the Heart of Texas Workforce Centers (WSHOT Center), and agency partners(partners). All hardware, software programs, and network technology are to be used for the purposes of creating, researching, and processing WSHOT -related materials. Users of the Board's resources are to be aware that they shall have no expectation of privacy for any activities performed on any of the Board's information resources.

All WSHOT Center staff, partners, volunteers, other agency representatives, and any other person granted access to the Board resources must comply with all standards set.

Software

All software acquired by or developed on the Board's behalf shall be deemed the Board's property unless otherwise agreed upon by management. All such software must be used in compliance with applicable licenses, notices, contracts, and agreements. Unauthorized access, disclosure, duplication, diversion, destruction, misuse, or theft of software is prohibited.

PURCHASING:

All requests for software purchases must be approved by the appropriate management staff **prior** to submission to the Information Technology (IT) Department. The IT Department shall review software requests to ensure that the technology requested conforms to the established standards. All requests to IT will be sent to the Board for approval. All software purchased becomes the Board's property and shall be centralized in the IT Department and will be available upon management request.

SOFTWARE STANDARDS:

Software standards are established by the Board and are subject to change without notice. WSHOT Center staff & partners shall not install **any** additional software products. This includes any "pop-up updates" to existing software. Any use of any unauthorized and/or unlicensed software is prohibited. Staff needing software other than the provided standard applications must be requested in writing and/or e-mail to the IT Department by the user's manager. Each request will be considered on a case-by-case basis in conjunction with the software purchasing section of this policy.

SOFTWARE USAGE:

Streaming Audio / Video (i.e. YouTube, Pandora, etc.) – No streaming audio or video may be used unless it is part of a TWC or WSHOT Board requirement.

Internet Websites – The Board has put a content filter in place that keeps employees and customers from going to websites that are not deemed permissible in a professional work environment. Internet surfing should be limited to job related sites and may be monitored.

Instant Messaging (i.e. Yahoo Chat, Skype) – No instant messaging software is to be used except through installed email and for business purposes only.

Social Media (i.e. Facebook, **Twitter)** – The use of "social networking" Internet sites by WSHOT Center users or partners is prohibited except as it is directly related to the functions of the user's job duties.

EXCEPTIONS:

All exceptions must be approved by the Heart of Texas Workforce Board Executive Director or designated board staff.

Network Resources

All referenced electronic mail and Internet connection systems are the sole property of the Heart of Texas Workforce Board, in conjunction with the Texas Workforce Commission's Information Systems. These systems and related resources are provided for the conduct of official Board, Contractor and Subcontractor's Workforce Development business.

Board and TWC management along with other authorized personnel may examine or inspect employee electronic and Internet communications where necessary for work related purposes, including situations in which Board and TWC management determines the need to investigate possible misconduct via either on-site or remote monitoring. Employees should be aware that many electronic communications constitute public records and must be retained. Files and applications from outside sources such as the Internet are subject to the security requirements found in the TWC Information System Security Agreement and may not be downloaded and installed on local computers or networks without prior authorization, without virus protection and detection review, and without proper licensing agreements. Employees will not use, load, install or operate shareware or freeware or other copyrighted or un-copyrighted software that has not been formally acquired and licensed by TWC and the Heart of Texas Workforce Development Board.

Confidentiality

All Board, Contractor and Subcontractor employees must read and sign the TWC Information System Security Agreement prior to obtaining an Email account.

E-mail and Internet

All electronic mail (e-mail) that is sent and received through the Workforce Board's e-mail servers is property of the Board and is subject to review upon board staff approval. All incoming and outgoing e-mail activity is monitored & archived. Any e-mail activity that is prohibited by this policy may not be allowed to pass through the e-mail server. The following activities are prohibited:

- Email account configuration on personal mobile devices (i.e. cell phones, tablets, & laptops) is prohibited. Email accounts are only to be configured on WFSHOT Board provided mobile devices (i.e. cell phones, tablets, & laptops). Exceptions must be approved by the Executive Director.
- Sending or receiving confidential or client PII unencrypted or not password protected
- Sending client PII information to unsecure or unauthorized email addresses
- Sending e-mail that is intimidating, abusive, bigoted or harassing
- Sending obscene or profane messages
- Sending Chain letter emails
- Using e-mail for personal reasons and/or for personal gain
- Using unauthorized e-mail software

E-mail messages with attachments greater than 10MB currently cannot be sent or received through our systems

Personal Use

<u>Generally, the content of electronic mail messages should be limited to official business.</u> <u>However, management recognizes that by using electronic mail to take care of some</u> <u>minor personal matters, employees may actually reduce the amount of time spent on such</u> <u>activities, devote more time to job tasks, and enhance employee productivity.</u> **The Board does permit incidental personal use of electronic mail systems.**

Access to the Internet is a privilege that may be revoked at any time for inappropriate use or conduct, including use that violates other applicable Board policies.

Employee Responsibilities

All employees assume responsibility for the content and dissemination of their messages. Electronic records constitute official records under the Open Records Act and may be available to the public. E-mails which reflect negatively on the individual may also reflect negatively on the Board and may result in legal liability for both.

Passwords

The Workforce Board has established guidelines for creating, changing, distributing, safeguarding, and terminating credentials for Heart of Texas Workforce (hotworkforce) domain network authentication. This policy excludes state applications such as TWIST, WIT, etc. which follow state guidelines. The policy is as follows:

- Passwords are to be a minimum of 8 alpha-numeric characters
- You will be prompted to change your password every 60 days
- You cannot use any of the last 3 previous passwords
- Your account will be locked out after 3 failed attempts for the duration of 30 minutes

Passwords are <u>not</u> to be shared with anyone. If you suspect someone may have your password, change it immediately.

Wi-Fi Access

Wireless access is provided for WSHOT Center and Board staff, partners & guests. Guests include those conducting job fairs, employers, and trainers providing services to WSHOT staff or clients. Guests do **NOT** include clients or the general public visiting any of the WSHOT sites. All internet traffic is monitored and is subject to review. All Wi-Fi users should expect no privacy when utilizing the Board's Wi-Fi access.

WSHOT Center staff are **NOT** to distribute guest Wi-Fi passwords to any guests. Any guest requests for access to network resources such as printers over Wi-Fi will need to have a staff member submit a help desk request to the IT Department.

File Shares

Network file shares are provided for the storage of Board & WSHOT Center business related documents. No personal files shall be stored on the network shares. All files stored on these network shares become the Workforce Board's property and are subject to review.

Any confidential or client files that contain Personal Identifiable Information (PII) stored on these network shares must be encrypted or password protected.

Hardware

All hardware devices acquired by the Workforce Board shall be deemed the Board's property. All such hardware devices must be used in compliance with applicable licenses, notices, contracts, and agreements. Any outside hardware must be approved by the IT Department. Any data stored on a desktop, laptop workstation, or tablet is the Workforce Board's property and may be subject to review. WSHOT Center staff shall not install **any** additional hardware products. Employees needing hardware other than the provided standard equipment must be requested in writing to the IT Department by the user's manager. Each request will be considered on a case-by-case basis in conjunction with the hardware purchasing section of this policy. Hardware standards are established by the Workforce Board and are subject to change without notice

PURCHASING:

All hardware purchasing requests, including telephone equipment, personal computers, and peripheral equipment, shall be reviewed and approved by the IT Department to ensure all equipment conforms to supported hardware standards. All requests for purchases must be approved by the appropriate immediate management staff prior to submission to the IT Department.

PERSONAL COMPUTERS & PRINTERS:

Since hardware standards become rapidly obsolete, purchases must be approved by the IT Department to ensure technology and equipment are at the top of the technology performance curve.

Desktop Computer Workstations – Provided to employees who work primarily from the office location with exceptions made for staff who have management approval to telecommute.

Laptop Computer Workstations/Tablets – Provided to employees required to frequently work away from the office, with management approval.

Printers – Access is given to all network laser printers. Management staff must approve any local printers.

Removable Media

The purpose of this policy is to define standards, procedures, and restrictions for end-users who have legitimate business requirements to connect portable removable media to any infrastructure within Workforce Board's internal network(s) or related technology resources. This removable media policy applies to, but is not limited to, all devices and accompanying media that fit the following device classifications:

- Portable USB-based memory sticks, also known as flash drives, thumb drives, jump drives, or key drives.
- Memory cards in SD, Compact Flash, Memory Stick or any related flash-based supplemental storage media.
- USB card readers that allow connectivity to a PC.
- Portable MP3 and MPEG-playing music and media player-type devices such as iPods with internal flash or hard drive-based memory that support data storage function.
- PDAs, cell phone handsets and Smartphone's with internal flash or hard drive-based memory that support data storage function.
- Digital cameras with internal or external memory support.
- Removable memory-based media, such as rewritable DVDs, CDs, and floppy disks.
- Any hardware that provides connectivity to USB devices through means such as wireless (Wi-Fi, WiMAX, IrDA, Bluetooth, among others) or wired network access.

All staff & partners have the overall responsibility for the confidentiality, integrity, and availability of corporate data.

All staff and partners have the responsibility to act in accordance with company policies and procedures. It is the responsibility of any Board staff, WSHOT Center employee or WSHOT Partner who is connecting a USB-based memory device to the organizational network to ensure that all security protocols normally used in the management of data on conventional storage infrastructure are also applied here. It is imperative that any portable memory that is used to conduct WFSHOT business be utilized appropriately, responsibly, and ethically. Failure to do so will result in immediate suspension of that user's account.

IT reserves the right to refuse, by physical and non-physical means, the ability to connect removable media and USB devices to corporate and corporate-connected infrastructure. IT will engage in such action if it feels such equipment is being used in such a way that puts the company's systems, data, users, and clients at risk.

WSHOT Center staff and partners must permanently erase company-specific data from such devices once their use is no longer required.

EXCEPTIONS:

Employees needing computer hardware other than the standard provided must first submit the request to their supervisor, and then the supervisor can forward the request to IT for approval by the Workforce Board Executive Director or designated board staff.

EQUIPMENT MOVES:

Equipment moves must be approved by management and a Help Desk ticket must submitted to the IT Department <u>prior</u> to the event.

VIOLATIONS AND PENALTIES:

Penalties for violating the Software/Hardware Policy vary depending on the nature and severity of the specific violation and are subject to:

- 1. Actions which are inconsistent with the provisions set forth in this policy and other applicable Board and Contractor policies may subject the employee to disciplinary action, including but not limited to reprimand, temporary or permanent suspension of privileges and/or termination of employment.
- 2. Civil or criminal prosecution under federal and/or state law.

YOU MUST SIGN AND RETURN THIS DOCUMENT

ACCEPTANCE:

Each user assumes personal responsibility for the appropriate use and agrees to comply with this policy, as well as any applicable city, state, and federal laws and regulations. I have read, understand and received a copy of the Heart of Texas Workforce Board and Workforce Centers Acceptable Use Policy.

PRINT NAME

SIGNED

DATE SIGNED

IT DEPARTMENT SIGNATURE

Systems Access and Data Security Report For Other Agencies and Community Partners – P-48 (0112)

Workforce Applications

INSTRUCTIONS: Within 10 days of providing, terminating, or adjusting access and permissions to Workforce Applications for staff from another agency or faith- or community-based organization, the Local Workforce Development Board (Board) must complete this form. The Board must ensure that the <i>TWC</i> <i>Information Resources Usage Agreement</i> (Form P-41) is completed, as appropriate. The originals are maintained at the Board offices and available upon request for review.				
Date: Access Report: New Adjusted Terminated			Terminated	
External Agency or Community Partner				
Organization Name: Address:				
	Access Au		A 1. /	
Name(s) of Individual(s)		Workforce Applications		
		View	Edit	
Justification for provid	ling access:			
Authorized Board Representative				
Name:	Title:	_		
Signature:Date:				

Texas Workforce Commission P-41 Information Resources Usage Agreement (0716) READ THE AGREEMENT CAREFULLY AND COMPLETELY BEFORE SIGNING. Last Name: First Name: Middle Name: Employee # / User ID: Work Phone with Area Code: Work Email: Employer / Cost Center: TWC Staff | DCS Staff | WDB Staff / Contractor Contractor Temporary Purpose This document informs you of your responsibilities concerning the use of Information Resources owned or held in trust by the Texas Workforce Commission (TWC). This agreement applies to anybody who needs access to these Information Resources or any state-owned or controlled Information Resources while making use of TWC owned or operated networks or connections. "Information Resources means the procedures, equipment, and software that are employed, designed, built, operated, and maintained to collect, record, process, store, retrieve, display and transmit information, and associated personnel including consultants and contractors." --TX. Govt. Code2054.003(7). For purposes of this agreement, Information Resources also includes Information Resources Technologies which are defined as data processing and telecommunications hardware, software, services, supplies, personnel, facility resources, maintenance, and training. --TX. Govt. Code 2054.003(8). **Confidential and Sensitive Information** As a user of TWC systems, you may have access to confidential or sensitive information through use of agency Information Resources or through your associated activities with agency information systems. Confidential and sensitive information includes: (1) Identifying information, (2) Federal Tax Information (FTI), (3) Office of Child Support Enforcement (OCSE) Federal Parent Locator Service (FPLS) National Directory of New Hires (NDNH) Information, (4) "Personally identifiable student information" under Family Educational Rights and Privacy Act (FERPA), (5) Texas Department of Insurance, Division of Worker's Compensation Information Data under Texas Labor Code §§ 402.082 - 402.092, (6) Personal health information, (7) Criminal justice information, and (8) Any information that is classified as confidential or sensitive by federal or state law or by agency policy, or is defined as a. "Personal Identifying Information" under Texas Business and Commerce Code §521.002(a)(1), or b. "Sensitive Personal Information" as defined by Texas Business and Commerce Code §521.002(a)(2). As a user of TWC systems, you are required to conform to applicable laws and agency policies governing confidential and sensitive information. You are required to read and abide by the obligations outlined throughout this document. I hereby certify that I have read, understand and agree to comply with all Initial: applicable laws, policies, standards and guidelines. Page 1 of 3

Authorized Use

I understand, acknowledge and agree that:

- (1) Information Resources are to be used for official state-approved business;
- (2) Information Resources are not for personal use;
- (3) I will not perform any work, review, update, or otherwise act to obtain information about my own, or any relative's, friend's or business associate's case, claim or account, even if it is closed;
- (4) There may be specific limited use exceptions outlined in other TWC policies and procedures;
- (5) TWC has a duty to protect its Information Resources;
- (6) TWC has the right to control or filter access to specific information resources;
- (7) TWC has the right to monitor the use of Information Resources under its authority;
- (8) TWC retains the right to terminate, restrict or limit access to or use of any Information Resources by any individual(s); and
- (9) Users of TWC Information Resources have no right to expect privacy in their use of Information Resources or in the content of their communications sent or stored in TWC owned or operated Information Resources.

User ID and Passwords

I understand, acknowledge and agree that:

- (1) I will receive and will be required to use one or more User IDs and/or Passwords to gain access to and to use Information Resources;
- (2) My User IDs and Passwords are security controls and must be used only by me; and

I will be held personally responsible for any actions taken by, or for any harm, loss, or adverse consequences arising from, the use of my User IDs and Passwords, including any unauthorized use by a third party if such party gains access to my User IDs and Passwords due to my negligence or misconduct; and such third party transactions will be considered as having been authorized and electronically signed by me.

Software

I understand, acknowledge and agree that:

- (1) Only properly licensed software approved by the agency may be used on TWC computers; and
- (2) Any use of software on TWC computers must be in accordance with the applicable software license agreement and all applicable TWC policies and procedures.

Access to Data

I understand, acknowledge and agree that:

- (1) Proper authorization is required for access to all data owned or held in trust by TWC except for data that is maintained for public access;
- (2) I may be granted access to Personally Identifiable Information (PII) as part of my job, and it is my duty to protect PII from exposure to all unauthorized parties;
- (3) I will NOT DISCLOSE or discuss any confidential and sensitive information with unauthorized individuals; and
- (4) I further understand that any data considered, or designated as, confidential and/or sensitive shall have the full protection of all codes, laws, rules, standards and guidelines appropriate to those data and the particulars of their use.

Security of Equipment

I understand, acknowledge and agree that Information Resources must not be removed from TWC property physically, electronically or through any other means without written authorization and prior approval of supervisory staff, and that if I have questions about the security of Information Resources, I may address them to my supervisor or the appropriate technical staff.

Initial:_____I hereby certify that I have read, understand and agree to comply with all applicable laws, policies, standards and guidelines.

Page 2 of 3

Reporting Security Incidents

I understand, acknowledge and agree that it is my responsibility to report any security incidents to my supervisor or TWC Information Security in a timely manner.

Acknowledgement

I understand, acknowledge and agree that:

- (1) I must comply with the policies concerning Information Resources set out in the <u>TWC</u> <u>Enterprise Information Security Standards and Guidelines</u> located on the TWC intranet, as well as any changes to those standards and guidelines;
- (2) Violation of any of these policies could result in disciplinary action up to and including termination of my employment and/or prosecution under one or more applicable statutes;
- (3) I am aware that criminal and/or civil penalties may apply for unauthorized disclosure of Federal Tax Information as outlined in the following United States Code references:
 - a. Title 26 USC Section 7213 UNAUTHORIZED DISCLOSURE OF INFORMATION provides that such disclosure shall be a felony punishable upon conviction by a fine of up to \$5,000.00, or imprisonment of up to 5 years, or both, together with the costs of prosecution and dismissal from employment.
 - b. Title 26 USC Section 7213a UNAUTHORIZED INSPECTION OF RETURNS OR RETURN INFORMATION provides that unauthorized inspection shall be a felony punishable upon conviction by a fine of up to \$1,000.00, or imprisonment of up to 1 year, or both, together with the costs of prosecution and dismissal from employment. Section 7213a applies to all unauthorized inspections of returns and return information, regardless of storage medium.
 - c. Title 26 USC Section 7431 CIVIL DAMAGES FOR UNAUTHORIZED INSPECTION OR DISCLOSURE OF RETURNS AND RETURN INFORMATION provides two damage computations. A prevailing plaintiff may recover the costs of the action plus the greater of (1) statutory damages of \$1,000 for each act of unauthorized inspection or disclosure or (2) the sum of actual damages plus, in the case of a willful inspection or disclosure, or an inspection or disclosure resulting from gross negligence, punitive damages.
- (4) I am aware of the penalty for misuse of information in the National Directory of New Hires: The Secretary of Labor shall require the imposition of an administrative penalty (up to and including dismissal from employment), and a fine of \$1,000, for each act of unauthorized access to, disclosure of, or use of, information in the National Directory of New Hires established under subsection (i) by any officer or employee of the United States who knowingly and willfully violates section 6103 of the Internal Revenue Code of 1986.
- (5) I understand and acknowledge that the Texas Department of Insurance (TDI) Data is confidential under Texas Labor Code §§ 402.082 - 402.092 and that if I should violate any of those statutory provisions I would be committing a criminal offense under Texas Labor Code §402.091 and may be charged with a Class A misdemeanor.

By signing this form, I affirm that I am accountable for my actions relating to Information Resources. I acknowledge that I must complete and annually renew all required TWC Information Security Training (or approved equivalent) and IRS Safeguards training. I have read and understand this document and agree to comply with this agreement and comply with all applicable laws, policies, standards and guidelines. I acknowledge that this form, in and of itself, does not grant or approve any access to the information discussed above.

Employee Signature:

Date:

I have discussed the need for strict confidentiality with the employee, have confirmed that he/she has completed the TWC Information Security Training (or approved equivalent) and IRS Safeguards Training, and fully understands the consequences of a violation of this agreement including U.S. Code violations.

Supervisor or Authorized HR Representative Name and Title:	Phone Number:
Supervisor or Authorized HR Representative Signature:	Date:
TWC P-41 (0716) Information Resources Usage Agreement – See P-41 Instruct	ctions for form routing information. An
individual may receive, review, and correct information collected at TW	/C about the individual by emailing
open.records@twc.state.tx.us or writing to TWC – Open Records Section, 101 E	ast 15 th St. Rm 266, Austin, TX 78778.

Page 3 of 3



WIT Access Request Form

First	Name:
Agen	icy:

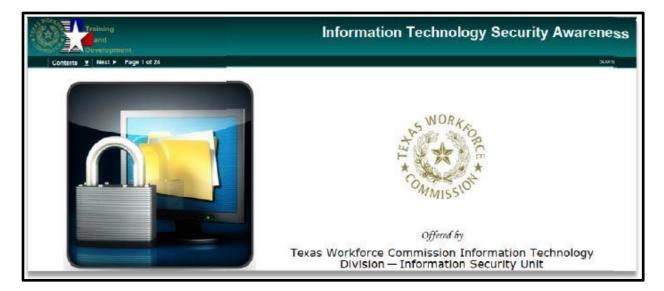
Last Name: Job Title:

Select Office Access:	Select Default Office Access:		
137 – WF SOL HOT Dev Bd	137 – WF SOL HOT Dev Bd		
140 – WF SOL HOT Waco	140 – WF SOL HOT Waco		
143 – WF SOL HOT Marlin	143 – WF SOL HOT Marlin		
145 – WF SOL HOT Hillsboro	145 – WF SOL HOT Hillsboro		
146 – WF SOL HOT Teague	146 – WF SOL HOT Teague		

Select Access Group:	Select Position Type:
Board LWDB - BSU Reps LWDB - Center Staff TVC / TVLP	DVOP (VESS) LVER (WWS)

Additional Privilege Request:

Employee Copy



<u>All</u>TWC, Board, and Contractor employees must complete the Information Technology Security Awareness Training prior to being granted access to TWC, HHSC, or Board systems, applications, or programs.

When completed print off (3) copies of your certificate. Include one copy with your completed security packet and give the second copy to your supervisor. Keep the third copy for your records.

To take your test and print off your certificate please go to the link provided below. Make sure once you have the test site loaded you enable "Compatibility View" in your Internet Explorer settings.

https://www.softchalkcloud.com/lesson/serve/FsewOymjL9GAbS/html

HEART OF TEXAS NOTICE Equal Opportunity Is the Law

The Heart of Texas Workforce Board, as a recipient of federal financial assistance, must provide the following notice that it does not discriminate on any prohibited ground.

EQUAL OPPORTUNITY IS THE LAW

It is against the law for this recipient of federal financial assistance to discriminate on the following bases: against any individual in the United States, on the basis of race, color, religion, sex (including pregnancy, childbirth, and related medical conditions, sex stereotyping, transgender status, and gender identity), national origin (including limited English proficiency), age, disability, or political affiliation or belief, or, against any beneficiary of, applicant to, or participant in programs financially assisted under Title I of the Workforce Innovation and Opportunity Act, on the basis of the individual's citizenship status or participation in any WIOA Title I-financially assisted program or activity. The recipient must not discriminate in any of the following areas: deciding who will be admitted, or have access, to any WIOA Title Ifinancially assisted program or activity; providing opportunities in, or treating any person with regard to, such a program or activity; or making employment decisions in the administration of, or in connection with, such a program or activity. Recipients of federal financial assistance must take reasonable steps to ensure that communications with individuals with disabilities are as effective as communications with others. This means that, upon request and at no cost to the individual, recipients are required to provide appropriate auxiliary aids and services to qualified individuals with disabilities.

WHAT TO DO IF YOU BELIEVE YOU HAVE EXPERIENCED DISCRIMINATION

If you think that you have been subjected to discrimination under a WIOA Title I–financially assisted program or activity, you may file a complaint within 180 days from the date of the alleged violation with either:

 the recipient's Equal Opportunity Officer (or the person whom the recipient has designated for this purpose); or Director, Civil Rights Center (CRC), US Department of Labor 200 Constitution Avenue NW, Room N-4123, Washington, DC 20210 or electronically as directed on the CRC website at www.dol.gov/crc.

If you file your complaint with the recipient, you must wait either until the recipient issues a written Notice of Final Action, or until 90 days have passed (whichever is sooner), before filing with the CRC (see address above). If the recipient does not give you a written Notice of Final Action within 90 days of the day on which you filed your complaint, you may file a complaint with CRC before receiving that notice. However, you must file your CRC complaint within 30 days of the 90-day deadline (in other words, within 120 days after the day on which you filed your complaint with the recipient). If the recipient does give you a written Notice of Final Action on your complaint, but you are dissatisfied with the decision or resolution, you may file a complaint with CRC. You must file your CRC complaint within 30 days of the date on which you received the Notice of Final Action.

If you wish to file a complaint, please ask for the Workforce Solutions Office manager, or contact:

Heart of Texas Workforce Board Aquanetta Brobston, EO Officer 801 Washington Ave, Suite 700 Waco, Texas 76701 254-296-5300/254-753-3173 Relay Texas: 711 or 1-800-735-2989 (TDD) 1-800-735-2988 (Voice)

Boone Fields, TWC EO Officer 101 E. 15th Street, Room 504 Austin, Texas 78778 (512) 463-2400 / Fax: (512) 463-7804 Relay Texas: 1-800-735-2989 (TDD) 1-800-735-2988 (Voice)



Auxiliary aids and services are available upon request to individuals with disabilities. Equal Opportunity Employer / Program

Keep this in your wallet/purse

Fold **CENTER CLOSURE PROCEDURES** WORK**SOLI** FORCE Notifications will be made via phone, social media and local news stations. Workforce Solutions Center Director will notify managers with instructions for staff. Workforce Solutions for the Heart of Texas Until then: **Employee Emergency Plan** · Check local news stations, Twitter & Facebook **QUICK TIPS** for updates: DO NOT make unnecessary telephone calls; WAIT to be contacted by your manager or by social media: MONITOR Internet Home Page (hotworkforce.com); **EMERGENCY NUMBERS** · If all communication is down, shelter in place EMERGENCY - 911 until further notice; KNOW your Alternative Location site; SHERIFF'S OFFICE • REPORT to work as directed or to the alternative Bosque County - (254) 435-2362 site: Falls County - (254) 833-1431 · Key Personnel follow your checklists. Freestone County - (903) 389- 3236 Hill County - (254)582 - 5313 REMEMBER Limestone County - (254) 729-3278 Do not make any public statement regarding the McLennan County - (254) 757-5000 situation. MCLENNAN COUNTY WACO POLICE (254) 750-7500 **ACTION** CONDITION IMPACT POINTS OF CONTACT Shelter-In-Place Hazardous Waste Center will close. Duck and Cover BOARD OFFICE Alert, Tornado, Severe Shelter in place Judy Hedge (w) 254-296-5300 or 254-296-5393 Weather until authorities issue "ALL CLEAR". On WEATHER PROTOCOL & SOCIAL MEDIA "ALL CLEAR," move Eunice Williams (w) 254-296-5324 to safe area. **PUBLIC MEDIA/** Intruder, Weapon, Center will close. **WORKFORCE SOLUTIONS CENTERS** Lock-Down David Davis (w) 254-296-5204 (c) 254-315-6370 Hostage, Active Shoot-Shelter in place er, Hostile Individual, until authorities issue **IT DEPARTMENT** Criminial Activity, "ALL CLEAR". On Tom McLain (w) 254-296-5213 (c) 254-644-9487 Dangerous Animal "ALL CLEAR," move to safe area. Matilda Alonzo (w)254-296-5212 (c)254-313-8355 Evacuate Fire, Explosion, Smell Take protective **BOARD STAFF** Building of Smoke/Gas. Fire measures for staff & Aquanetta Brobston (w) 254-296-5385 Alarm, Bomb Threat assets. (c) 254-424-4935

Kary Kuecker (w) 254-296-5381

The Heart of Texas Workforce Development Board, Inc. is an equal opportunity employer/ program and auxiliary aids and services are available upon request to include individuals with disabilities. TTY/TDD via RELAY Texas service at 711 or (TDD) 1-800-735-2989 / 1-800-735-2988 (voice). Fold

Fold

Fold

A proud partner of the AmericanJobCenter network