WORKFORCE SOLUTIONS
★★★ HEART OF TEXAS ★★★
Linking Jobseekers and Employers

User Access Request

Name:		
Date:	**Office #:**	**Workstation Name:**
Position:	**Manager:**	

■ New User	☐ Access Change / Transfer	☐ Annual Update

Department:

☐Board Staff	☐BSU	■Career Center	☐CCS
☐Choices/Snap	☐CIS	☐UI	☐Veteran Services
☐WIOA	☐WFC Management	☐Other:_____	

User Access: (Check all that apply)

☑Phone Ext. _____	■Network Access (Windows)	■Shared Network Drive	■Outlook Email
■WorkInTexas	☐TIERS	☐TWIST	☐RAC-F Mainframe
■WSHOT Intranet	■LinkedIn Learning	■Infosec Training	■Staff Newsletter
☐CCS Workflow	☐CCS Eligibility Calc	☐CCS Adobe DC	☐TABE
List other access needed:			

Management Approval
Signature: _____ Date: _____

NOTE:
Please be sure to complete ALL forms for access requests. Attach appropriate change forms for access change requests. All forms can be found on the Shared Drive.

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 staff member's manager. Each request will be considered on a case-by-case basis in conjunction with the software purchasing section of this policy.

INTERNET SOFTWARE USAGE:

Websites – A content filter is in place to protect employees and customers from going to websites that are malicious and can cause harm to the WSHOT technology infrastructure. Use caution when visiting various websites. All internet usage will be monitored.

Streaming Video (i.e. **Netflix**, **Hulu** etc.) – No personal TV/Movie streaming services may be used. Streaming video services such as YouTube may be used only for WSHOT business purposes. All streaming connections will be monitored.

Collaboration Software (i.e. **MS Teams, Zoom**) – Collaboration software is to be used for WSHOT business purposes only. Only WSHOT approved collaborations software should be used.

Social Media (i.e. Facebook, Twitter) – The use of social networking sites should be used with caution.

EXCEPTIONS:

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

Network Resources

All referenced e-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 devices.
- Sending 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 malicious, obscene or profane messages
- Using e-mail for personal gain
- Using unauthorized e-mail software

EXCEPTIONS:

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

Personal Use

Cloud platforms such as Google Chrome, Microsoft Edge, Adobe DC, etc. allows users to log in from anywhere that has internet connection and syncs all data to the device. Use caution when connecting to these products with personal logins. Once connected to WSHOT provided device, all data from that connection becomes the property of the Heart of Texas Workforce Development Board. Using WSHOT provided logins to these products is prohibited from use on personal devices.

The Board does permit incidental personal use of internet access.

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 12 alpha-numeric characters including a special character
- You will be prompted to change your password every 90 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 not to be shared with anyone. If you suspect someone may have your password, notify IT and change it immediately.

Wi-Fi Access

Staff Wi-Fi - Staff wireless internet access (HOTWF Staff) is provided for WSHOT Center and Board staff, contractors, and partners. All internet traffic is monitored and is subject to review. All Wi-Fi users should expect no privacy when utilizing the Staff Wi-Fi access.

Guest Wi-Fi - Guest wireless internet access (HOTWF Guest) is provided for WSHOT staff, contractor, and partner 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 Wi-Fi users should expect no privacy when utilizing the Guest Wi-Fi access.

Public Wi-Fi - Public wireless internet access (HOTWF Public) is provided for general public visiting any of the WSHOT sites. This wireless internet connection is NOT secure and WSHOT issued devices should NOT use this internet connection for any business activities.

WSHOT Center staff are NOT to distribute 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 including cloud storage are provided for 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 Informations (PII) stored on these network and/or cloud shares must be encrypted or password protected.

Hardware

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 management staff prior to submission to the IT Department.

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 to WSHOT network printers is provided. Local desktop printers are only provided upon approval by the Heart of Texas Workforce Board Executive Director or designated board staff.

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.
- Cellular Smartphones 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.
- Any hardware that provides connectivity to USB devices through means such as wireless (Wi-Fi, WiMAX, IrDA, Bluetooth, etc.) or wired network access.

All staff & partners have the overall responsibility for the confidentiality, integrity, and availability of corporate data. You have the responsibility to act in accordance with company policies and procedures.

It is your responsibility to ensure that all security protocols normally used in the management of data are also applied here. It is imperative that any portable memory device 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 manager, and then the manager 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 prior 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:

You agree to assume personal responsibility for the appropriate use and agree 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

HEART OF TEXAS WORKFORCE DEVELOPMENT BOARD, INC.

NONDISCLOSURE AGREEMENT

ID NO.:	HWD CS 005-22	**DATE ISSUED:**	9/1/2022
PROGRAM:	Cybersecurity	**KEYWORD:**	Non-Disclosure Agreement

1. Agreement Overview

This Nondisclosure Agreement is made and entered into as of ___/___/___ (the "Effective Date") between the Heart of Texas Workforce Development Board ("HOT"), located at 801 Washington Ave #700, Waco, TX 76701 and _____,located at 1416 S. New Road Waco TX 76711. Both organizations desire to disclose to each other Proprietary Information (as defined in Section 2.1) relating to possible business opportunities and teaming for future contracts (the "Purpose").

Now, therefore, in consideration of the foregoing and the mutual promises herein contained, Heart of Texas Workforce Development Board and _____ (the "Parties") agree as follows.

2. Duties and Exceptions

2.1 "*Proprietary Information*" defined. *Proprietary Information* shall mean all confidential proprietary or non-public information, whether written, oral, electronic, graphic, web-based or otherwise, directly or indirectly furnished or disclosed by one party or its affiliates to, or otherwise learned by, the other party or any of its subsidiaries or affiliates, including without limitation: information related to the operations of the disclosing party's business; information related to the relationships and contracts the disclosing party has with its employees, clients, vendors, suppliers, service providers, and other like persons; information related to the owners or partners of the disclosing party; information related to the relationships and contracts the owners or partners the disclosing party has with their employees, clients, vendors, suppliers, service providers; plans or proposals; marketing strategies; data; research; trade secrets; financial information; business polices or processes; pricing information; customer information; supplier/vendor information; processes; and any other information which, under the circumstances surrounding disclosure ought to be treated as confidential. Proprietary Information may be marked or otherwise designated as "Proprietary Information," but the parties do not have to mark or otherwise designate Proprietary Information as such.

2.2 Duty to protect and appropriately use Proprietary Information. The Parties each will employ reasonable efforts to keep in confidence and prevent disclosure of all Proprietary Information each receives from the other. Neither of the Parties will use Proprietary Information for purposes other than the Purpose.

2.3 Duty to properly label Proprietary Information. Any written material labeled Proprietary Information must be believed in good faith by the disclosing party to contain Proprietary Information. However, such information does not need to be marked in order for such information to be designated as Proprietary Information.

2.4 Duty to notify. The receiving party will notify the disclosing party in writing immediately upon the occurrence of any unauthorized release of Proprietary Information, whether inadvertent or otherwise, and will use reasonable efforts to prevent or limit any further dissemination.

2.5 Exceptions. Neither party will be liable for disclosure or use of information if the information is:

a. in the public domain at the time of disclosure, or is subsequently made available to the general public without restriction by the disclosing party;

b. known to the receiving party at the time of disclosure without restrictions on its use or independently developed by the receiving party without the breach of this Agreement, and there is adequate documentation to demonstrate either condition;

c. used or disclosed with the prior written approval of the disclosing party;

d. disclosed without restriction to the receiving party from a source other than the disclosing party who is not under any obligation of confidentiality with respect to such information; or

e. in the event any governmental or judicial order requires the disclosure of Proprietary Information, if the recipient of such Proprietary Information provides prompt written notice to the originator of the Proprietary Information of the requirement and provides reasonable aid and assistance if the originator decides to oppose such governmental or judicial order.

2.6 Survival. If any portion of either of the Parties' Proprietary Information falls within any one of the above exceptions, the remainder will continue to be subject to the foregoing prohibitions and restrictions. Furthermore, all obligations pursuant to the Proprietary Information shall survive any change or termination of this agreement or of the Parties' business relationship.

3. Standards of Protection

Each of the Parties will protect the Proprietary Information of the other party using the same degree of care, to prevent the unauthorized use, dissemination or publication of the confidential information as that party uses to protect its own Proprietary Information of comparable importance, but no less than a reasonable degree of care.

4. Remedies

4.1 Equitable relief. Each party acknowledges and agrees that, due to the unique nature of the other party's Proprietary Information, remedies at law may be inadequate to protect the disclosing party against the potentially irreparable harm resulting from an actual or threatened breach of this Agreement by the receiving party. Therefore, upon any such breach or any threat thereof, the disclosing party will be entitled to seek appropriate equitable relief, including injunctive relief and specific performance, in addition to any other rights and remedies the disclosing party might have at law.

4.2 No punitive or multiple damages. In no event will either party be liable hereunder or otherwise for punitive or multiple damages.

4.3 Attorneys' fees. The disclosing party will be entitled to reasonable attorneys' fees and other costs incurred to remedy any breach.

4.4 Indemnity. The disclosing party further agrees to indemnify and hold the receiving party harmless from all injury, loss, or damage that may arise out of or result from a breach of this representation.

5. Designated Agents

The sole designated agents of the Parties authorized to receive written Proprietary Information are:

6. Notice to Party Employees
Prior to disclosure of Proprietary Information to any employee, each party will fully advise such employee that he or she is required to hold in confidence all information and that such information is not to be disclosed to persons outside his or her organization or to any co-employee not directly concerned with furthering the Purpose. The Parties will maintain between themselves and their officers, employees, and consultants duly binding agreements as may be necessary to fulfill obligations under this Agreement.

7. Termination
7.1 Return or destruction of Proprietary Information. All documents, drawings, and writings disclosing Proprietary Information and all copies thereof will be returned promptly by a party to the other party, or will be destroyed and a written certificate of destruction provided, upon receipt of a request therefore or following termination or expiration of this Agreement.

7.2 Voluntary termination. This Agreement may be terminated at any time by either party giving 30 days prior written notice to the other party.

7.3 Automatic termination. Unless earlier terminated, this Agreement will expire one year from the Effective Date.

7.4 Effect of termination on Proprietary Information. Any information exchanged after such termination or expiration will not be considered Proprietary Information. The Parties' obligation to protect Proprietary Information will survive any such expiration or termination.

8. Representations and Warranties
8.1 No rights or obligations other than those expressly recited herein will be implied from this Agreement.

8.2 The disclosure of Proprietary Information hereunder will not be construed as granting either a license under any patent or patent application or any right of use or ownership in said Proprietary Information. Nor will such disclosure constitute any representation, warranty, assurance, guarantee or inducement by the disclosing party with respect to infringement of patents or rights of third parties.

8.3 No warranty or representation as to the accuracy, completeness or technical or scientific quality of any Proprietary Information is provided herein.

8.4 Without restricting the generality of the foregoing, the Parties make no representation or warranty as the merchantability or fitness for a particular purpose of any Proprietary Information disclosed hereunder.

8.5 The disclosing party represents that it has the right to disclose all information transmitted to the receiving party under this Agreement.

9. Merger
This Agreement merges all prior discussions and is the entire understanding and agreement of the parties relating to the protection of Proprietary Information; neither party will be bound by any additional or other representation, condition, or promise except as subsequently set forth in a writing signed by the party to be bound.

10. Confidentiality of this Agreement

Neither party will announce or communicate any information concerning this Agreement to any third party, without the prior written approval of the other party.

11. Export Control Laws
The Parties will adhere to any applicable U.S. and foreign export control laws and regulations and will not export or re-export any technical data or products received or the direct product of such technical data except in compliance with the applicable export control laws and regulations of the U.S. and any foreign country.

12. Severability
If any portion of this Agreement is held to be unenforceable, the unenforceable portion will be construed as nearly as possible to reflect the original intent of the parties, the remaining portions remain in full force and effect, and the unenforceable portion remains enforceable in all other contexts and jurisdictions.

13. Headings and Plural Terms
The section headings contained in this Agreement are for reference purposes only and do not affect in any way the meaning or interpretation of this Agreement. Terms defined in the singular have the same meaning in the plural and vice versa.

14. Governing Law
The validity and interpretation of this Agreement will be governed by the laws of the State of Texas, U.S.A., applicable to agreements made and to be performed wholly within such jurisdiction. The Parties hereto agree that the exclusive jurisdiction for any claim or suit brought to enforce a party's rights under this Agreement shall be thecourts of the State of Texas and that venue shall be any court of the State of Texas in McLennan County, Texas, and the Parties hereby waive any claim that McLennan County, Texas is an inconvenient forum.

15. Agreement Approval
In witness whereof, duly authorized representatives of the undersigned parties have executed this Nondisclosure Agreement as of the Effective Date.

Heart of Texas Workforce Development Board	
	Organization Name
Date:	
	Date:
By: _____	By: _____
Print Name:	Print Name:
Print Title:	Print Title:

Texas Workforce Commission

P-41 Information Resources Usage Agreement (02/23)

Please read the agreement carefully and completely before signing.

First Name:	MI:	Last Name:
Employee #/User ID:	Work Phone:	
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. Code 2054.003(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) Federal Tax Information (FTI),
(2) Office of Child Support Enforcement (OCSE) Federal Parent Locator Service (FPLS) National Directory of New Hires (NDNH) Information,
(3) "Personally identifiable student information" under Family Educational Rights and Privacy Act (FERPA),
(4) Texas Department of Insurance, Division of Worker's Compensation Information Data under Texas Labor Code §§ 402.082 - 402.092,
(5) Personal health information,
(6) Criminal justice information, and
(7) 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).

Authorized Use:

I understand, acknowledge and agree that:

(1) Information Resources are to be used only 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) Use of personal devices to conduct state business, including accessing any state-owned data, applications, email accounts, or non-public facing communications, is prohibited under the Statewide Plan to Prevent the Use of Prohibited Technologies ; and
(10) Users of TWC Information Resources have no right to 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.

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.

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.

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, and standards appropriate to those data and the particulars of their use.

Acknowledgement:

I understand, acknowledge, and agree that:

(1) I must comply with the policies concerning Information Resources set out in the TWC Information Security Manual and guidelines located on the TWC intranet, as well as any changes to those policies, 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.

Acknowledgement Continued:

(6) Intellectual Property: I acknowledge that the source codes, programs, and related documentation constitute valuable intellectual property for the agency. I understand and agree that I may have access to intellectual properties (trademarks, patents, trade secrets, and materials and documents) belonging to TWC. I understand and agree that these properties made available to me are confidential and protected by intellectual property laws. These properties are not to be disclosed, copied, or shared with any unauthorized person(s) without the written permission of TWC. I understand and agree that I may be required to develop, create, or modify materials protected by intellectual property laws and that this work is solely the intellectual property of TWC and may not be disclosed, copied, or shared with unauthorized person(s) without the written permission of TWC. I understand that using TWC's intellectual property for other than their intended purposes is prohibited and may result in termination of employment and prosecution pursuant to Texas Penal Code §31.05, as well as TWC's pursuit of any other legal remedies.

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, and standards. I acknowledge that this form, in and of itself, does not grant or approve any access to the information discussed above.

Employee Signature:	**Date:**

TWC P-41 (02/23) Employee Information Resources Usage Agreement.
See P-41 Instructions for additional information on form routing.

An individual may receive, review, and correct information collected at TWC about the individual by emailing open.records@twc.state.tx.us or writing to TWC Open Records Section, 101 East 15th St. Rm 266, Austin, TX 78778.

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 *TWC Information Resources Usage Agreement* (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

External Agency or Community Partner

Organization Name: Workforce Solutions for the Heart of Texas
Address: 1416 S. New Road, Waco TX 76711

Access Authorized

Name(s) of Individual(s)	**Workforce Applications**	
	View	**Edit**
_____	☑	☑
_____	☐	☐
_____	☐	☐
_____	☐	☐

Justification for providing access:

_____ provide customer service

Authorized Board Representative

Name:_____	Title: _____

Signature:_____ Date: _____

WORK FORCE SOLUTIONS
★★★ HEART OF TEXAS ★★★
Linking Jobseekers and Employers

WIT Access Request Form

First Name: Arturo
Last Name: Torija
Agency: Workforce Solutions for the
Job Title: WDS I

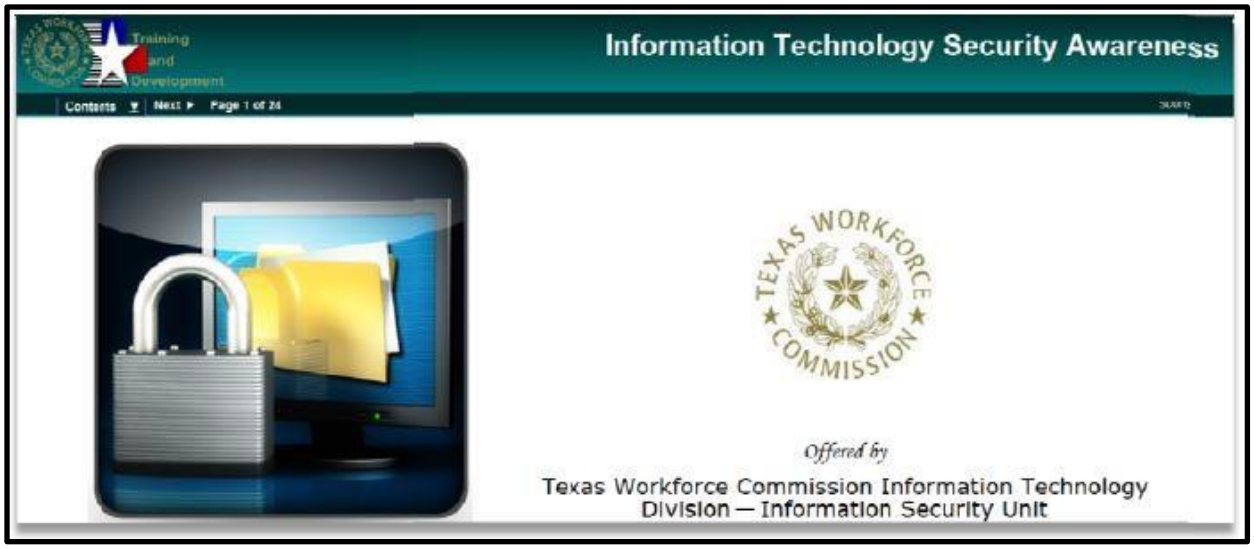
Select Office Access:	**Select Default Office Access:**
☐137 – WF SOL HOT Dev Bd	☐ 137 – WF SOL HOT Dev Bd
☐140 – WF SOL HOT Waco	☐ 140 – WF SOL HOT Waco
☐143 – WF SOL HOT Marlin	☐ 143 – WF SOL HOT Marlin
☐145 – WF SOL HOT Hillsboro	☐ 145 – WF SOL HOT Hillsboro
☐146 – WF SOL HOT Teague	☐ 146 – WF SOL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

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

Additional Privilege Request:

Supervisor: _____ Date: _____

Employee Copy



<u>All</u> TWC, Board, and Contractor employees must complete the CyberSecurity Awareness and the Sensitive Personal Information 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/EbzdcZtNkrB0Lq/html

https://www.softchalkcloud.com/lesson/serve/GCcx9Dsuk3jheW/html

HEART of TEXAS N O T I C E

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 I–financially 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