PWDB
Cybersecurity Council
Meeting Agenda
May 24, 2023

PANHANDLE REGIONAL PLANNING COMMISSION

NOTICE OF MEETING

A meeting of the Panhandle Workforce Development Board's Cybersecurity Council will be held at 11:45 a.m. on Wednesday, May 24, 2023. Due to the COVID-19 crisis, this meeting will be held in hybrid format with videoconference available pursuant to Texas Government Code Section 551.127.

Under the hybrid format, Council members and individuals from the public may access the meeting in person at 3120 Eddy Street, Amarillo, Randall County, Texas. Lunch will be served to Council members beginning at 11:30 a.m.

Council members and individuals of the public interested in attending this meeting by videoconference may do so by logging onto:

https://us02web.zoom.us/j/81140045418?pwd=NlBNQVlKTTdHVStXSzhqanAvQzYydz09 (Meeting ID 811 4004 5418 Passcode: 561282);

Or may participate by phone (346) 248-7799 (Meeting ID: 811 4004 5418 Passcode: 561282).

A copy of the agenda for this meeting can be found on the PRPC's website at http://www.theprpc.org

The Cybersecurity Council shall provide an opportunity for oral comments from the public during the meeting. Each person wishing to make a public comment shall be limited to three (3) minutes and limited to speaking once per comment period. Comments shall be directed to the Council as a whole. Individual Council members will not respond to questions. In the event that a group of persons supporting/opposing the same position desires to be heard, in the interest of time, a spokesperson shall be designated to express the group's position.

AGENDA

1. **CALL TO ORDER**

2. **INITIAL PUBLIC COMMENT PERIOD**

3. **MINUTES**

   Members will be asked to consider approval of the minutes from the Council's meeting held on February 22, 2023.

415 South West Eighth Avenue
P. O. Box 9257
Amarillo, Texas 79105
(806) 372-3381
(806) 373-3268 (fax)
www.theprpc.org

**** AT THIS POINT IN THE MEETING, MEMBERS WILL ENTER A BRIEF CLOSED SESSION ****

as per Texas Government Code §551.089, which does not require a governmental body to conduct an open meeting to deliberate:

(a) security assessments or deployments relating to information resources technology;

(b) network security information as described by §2059.055(b) ; or

(c) the deployment, or specific occasions for implementation, of security personnel, critical infrastructure, or security devices.

4. **PANHANDLE WORKFORCE DEVELOPMENT BOARD (PWDB) SECURITY AND CYBERSECURITY POLICY**

   Members will be presented with one new and one updated proposed PWDB Security and Cybersecurity policy for discussion and input. No action by the Council will be taken in the closed session.

   - Technology Equipment – Devices and Prohibited Technologies
   - Systems and Applications – Systems Access

**** AT THIS POINT IN THE MEETING, MEMBERS WILL RETURN TO THE OPEN SESSION****

5. **VOTE ON PWDB SECURITY AND CYBERSECURITY POLICY**

   Members will be asked to vote on the proposed PWDB Security and Cybersecurity policies described in the previous item. The results of the discussion, input and subsequent vote will be reported to the full PWDB at its May 24th, 2023 meeting immediately following the Cybersecurity Council meeting.

6. **OPEN DISCUSSION**

   Members have the opportunity to discuss topics of interest. No action by the Council is required.

7. **CURRENT MEMBERSHIP LIST**

   Informational item only. No action by the Council is required.

8. **FINAL PUBLIC COMMENT PERIOD**

9. **ADJOURN**

PUBLIC NOTICE

This notice complies with Texas Government Code Chapter 551, Open Meetings Act, Section 551.041 (Notice of Meeting Requirements); Section 551.043 (Time and Accessibility of Notice Requirements); and Section 551.053 (Notice Requirements of a Political Subdivision Extending into Four or More Counties). The notice has been filed at least 72 hours before the scheduled time of the meeting with the Secretary of State's Office, the Potter County Clerk's Office and has been posted in the Administrative Office of the Panhandle Regional Planning Commission.

Posted this 18th day of May 2023, at 415 Southwest Eighth Avenue, Amarillo, Texas, at 11:00 a.m.

Leslie Hardin

Leslie Hardin

PANHANDLE
REGIONAL
PLANNING
COMMISSION

ITEM 3

PANHANDLE REGIONAL PLANNING COMMISSION

PANHANDLE WORKFORCE DEVELOPMENT BOARD

Cybersecurity Council

Minutes

February 22, 2023

A meeting of the Panhandle Workforce Development Board's Cybersecurity Council was held at 11:45 a.m. on Wednesday, February 22, 2023. Due to the current COVID-19 crisis this meeting was held in hybrid format by videoconference pursuant to Texas Government Code Section 551.127. Board members and individuals from the public who desired to attend in person, accessed the meeting at 3120 Eddy Street, Amarillo, Randall County, Texas.

Mr. Michael Wright, presided.

COUNCIL MEMBERS PRESENT:

- Texas "Tex" Buckhaults, Clarendon College
- Paul Salazar, West Texas Electrical Joint Apprenticeship & Training Committee
- Michael Wright, Moore County News – Press
- Magi York, Panhandle Community Services

COUNCIL MEMBER ABSENT:

None.

STAFF CYBERSECURITY COMMITTEE PRESENT:

Kathy Cabezuela, Ana Gonzalez, Leslie Hardin, and Marin Rivas, Panhandle Regional Planning Commission (PRPC); Trent Morris and Andrew Thompson, Workforce Solutions Panhandle (WSP).

OTHERS PRESENT:

None.

1. CALL TO ORDER

   Mr. Wright called the meeting to order noting that a quorum was present.

2. INITIAL PUBLIC COMMENT PERIOD

   None.

3. MINUTES

Members considered approval of the minutes from the Council's January 18, 2023 meeting. Ms. York moved to approve the minutes as presented. Mr. Buckhaults seconded the motion; the motion carried.

4. PANHANDLE WORKFORCE DEVELOPMENT BOARD (PWDB) CYBERSECURITY POLICIES

Members were asked to vote on three (3) PWDB Cybersecurity policy updates and one (1) new policy discussed in the closed session of the previous meeting:

a) Acceptable Use of Information Technology Resources - Update
b) Secure Configuration - Update
c) Risk Assessment and Mitigation - Update
d) Incident Response - New

Mr. Buckhaults made a motion to approve the updated and new policies. Ms. York seconded the motion; the motion carried. The record of the vote was recognized in the following PWDB meeting also held on February 22nd, 2023.

5. OPEN DISCUSSION

Members had the opportunity to discuss topics of interest. No action by the Council was required.

6. FINAL PUBLIC COMMENT PERIOD

None.

7. ADJOURN

There being no further business to come before the Board, Ms. York moved that the meeting adjourn. Mr. Salazar seconded the motion; the meeting adjourned.

PANHANDLE
REGIONAL
PLANNING
COMMISSION

ITEM 4

PANHANDLE WORKFORCE DEVELOPMENT BOARD MANUAL
Chapter 9-Technology Equipment
Section 9.1 Devices and Prohibited Technologies Effective 5-24-2023

PURPOSE:
To establish Panhandle Workforce Development Board policy with guidance on managing technology-enabled devices (i.e., cell phones, laptops, tablets, desktop computers, or any other devices capable of Internet connectivity) to protect sensitive information and critical infrastructure from prohibited technologies that have surveilling capabilities and/or pose a potential security threat; and identifying sensitive locations, meetings, or personnel that could be exposed to prohibited technology-enabled devices. This policy applies to all staff of the Panhandle Workforce Development Board (PWDB), Workforce Solutions Panhandle (WSP), the Texas Workforce Commission (TWC), Texas Veterans Commission (TVC) staff, and other community agencies and third-party partners.

BACKGROUND:
On December 7, 2022, Texas Governor Greg Abbott directed all State agencies in Texas to ban the video-sharing application TikTok over the Chinese Communist Party's (CCP) ability to use the application for surveilling Texans. The Governor directed agencies, including their employees, contractors, interns, or any users of State-owned networks, to develop a plan providing guidance to ban, and prevent the download, or use, of prohibited technologies; implement network-based restrictions to prevent the use of prohibited technologies; and to prevent prohibited technology-enabled devices from entering or being used in sensitive areas. TWC has issued and updated guidance in Workforce Development (WD) Letter 29-22, as amended, *Ban of TikTok and Other Nonwork-Related Social Network Services.*

The governor announced the Statewide plan providing State agencies guidance on managing technology-enabled devices used to conduct state business, *Model Security Plan for Prohibited Technologies,* developed by the Texas Department of Public Safety (DPS) and the Texas Department of Information Resources (DIR), https://dir.texas.gov/sites/default/files/2023-02/Statewide_Plan_for_Preventing_Use_of_Prohibited_Technology_in_State_Agencies_%28Final_OOG%29.pdf, and directed state agencies to implement their own policies.

TWC has adopted the *Prohibited Technologies Security Policy*, which can be found at https://www.twc.texas.gov/files/policy_letters/attachments/29-22-ch1-att2-twc.pdf, to align with the guidance from the governor.

DIR will maintain an up-to-date list of prohibited technologies, including applications, software, hardware, or technology providers, and provide recommendations to State leaders on technologies that must be blocked. The current list of prohibited technologies is available on DIR's website at https://dir.texas.gov/information-security/prohibited-technologies.

PANHANDLE WORKFORCE DEVELOPMENT BOARD (PWDB) POLICY:
Access to computer systems, equipment, State and local automated systems, and Workforce applications will only be provided to staff who need the information to perform their jobs, and to staff from other agencies or community partners, whose required forms have been received by the PWDB's Board Administrators. WSP and PWDB staff are responsible for protecting Personally

Identifiable Information (PII) and other sensitive information from unauthorized disclosure; complying with the requirements of the National Institute of Standards and Technology (NIST) and, as applicable, cybersecurity and information security industry "best practices".

It is the policy of TWC and the PWDB to protect the information resources in accordance with the Texas Administrative Code (TAC) Title 1, Part 10, Chapter 202, Subchapter B Information Security Standards and the Texas Government Code Chapter 2054, Information Resources Management Act, which outlines the minimum information security and cybersecurity responsibilities and roles at State agencies. TWC requires the PWDB to protect and maintain the security of information resources in accordance with applicable federal and State Rules and Regulations. At all times, all staff must prioritize data security and take all necessary and appropriate measures to ensure sensitive and confidential information is adequately protected. Staff must protect these assets against unauthorized access, disclosure, modification or destruction, whether accidental or deliberate, as well as assure the availability, integrity, utility, authenticity and confidentiality of information.

Board/Contractor-Issued Systems/Devices

The use of TikTok and all other prohibited technologies, on all PWDB/WSP-issued systems and devices, is banned, as PWDB/WSP has access to sensitive material that could potentially be made available to those databases. If TikTok or any other prohibited technology, is currently installed on any such systems/devices, it must be removed immediately.

PWDB/WSP staff are prohibited from installing or operating prohibited applications or technologies on any device used to conduct State business. State business includes accessing any State-owned data, applications, nonpublic facing communications, and email accounts; or State network resources including work email, Voice over Internet Protocol (VoIP), Short Message/Messaging Service (SMS); video conferencing (including, but not limited to, ZOOM Video Communications and Microsoft Teams Video Communications applications), the WSP website or portal; Centralized Accounting and Payroll/Personnel System (CAPPS); the official website of the State of Texas (Texas.gov); and any other State databases or applications.

Staff needing to conduct State business on a technology-enabled device must have PWDB/WSP management approval prior to utilizing any device or infrastructures, including Local Area Networks (LAN); Wide Area Network (WAN) or Virtual Private Network (VPN) connections; and MiFi mobile "hotspot" or other cellular wireless "hotspot" devices. Board/Contractor-issued devices and infrastructures may be provided, on an as-needed basis, as determined by PWDB/WSP management prior to individual personal staff use.

Personally-Owned Technology Devices

PWDB/WSP/TWC/TVC staff, and other community agencies and third-party partners, are prohibited from using any personally-owned device to conduct State business, including personal cell phones; laptop, tablet and desktop computers; MiFi mobile "hotspot" or other cellular wireless "hotspot" devices, or any other device capable of Internet connectivity.

While possession of personally-owned staff devices is not prohibited in PWDB/WSP locations, staff must ensure that technology-enabled, personally-owned staff devices with prohibited technologies installed are not allowed in any posted sensitive location or workspace (including

off-site or home workspaces), in the same room, or within "earshot" (a distance of no less than six (6) feet), of State business potentially being conducted.

Sensitive Location Identification

WSP management must identify, catalog, and label Sensitive Locations within WSP offices, Mobile Workforce Development Services Units, and home-based workstations. Notices of the Sensitive Locations must be posted.

A Sensitive Location is any location—physical or logical (such as video conferencing or electronic meeting rooms)—that is used to discuss confidential or sensitive information, including information-technology configurations, personally-identifiable data, sensitive personal information, or any data protected by federal or State law. Staff personally-owned devices, such as cell phones, tablets, or laptops with prohibited applications or technologies, may not enter sensitive locations, which includes any electronic meeting labeled as a sensitive location.

Sensitive locations include, but may not be limited to:

- In the WSP Amarillo office, the access-controlled secured area, and cubicles in the resource room;
- In the WSP Borger office, cubicles in the resource room;
- On the WSP Hereford site, the designated WSP staff office;
- The WSP Mobile Workforce Development Services Units; and
- A work-from-home workspace (same room or within "earshot").

Staff must ensure that technology-enabled personally-owned staff devices with prohibited technologies installed are not allowed in any posted sensitive location or workspace (including off-site or home workspaces), in the same room, or within "earshot". Staff must only discuss confidential or sensitive information in the designated and posted Sensitive Locations, and maintain a reasonable volume of the conversation to ensure others or devices are not able to hear or capture the conversation.

Network-Based Restrictions

In compliance with:

(1) TWC Agency Board Agreement (ABA), Attachment C, *Board Guidelines for Security*, which provides guidelines for the minimum acceptable standards for the Texas Cybersecurity Framework control objectives to ensure the security of TWC data entrusted to the Board, and

(2) Considerations in Objective #2 of the statewide *Model Security Plan for Prohibited Technologies*, which states that agencies will "Prohibit employees or contractors from conducting state business on prohibited technology-enabled devices", the WSP Information Technology (IT)/Cybersecurity Officer(s)/Systems Administrator(s) staff will:

- Implement network-based restrictions to prevent the use of prohibited technologies on agency networks by any prohibited technology-enabled device;
- Configure agency network firewall(s) to block prohibited domains on local networks, Wi-Fi Protected Access Networks (WPNs) and VPNs;
- Implement a mobile device management platform that prevents conducting business related to TWC programs, including accessing any State-owned data, applications, nonpublic facing communications, and email accounts; or State network resources

including State email, VoIP, SMS, video conferencing, and any other State databases or applications, on prohibited technology-enabled devices; and

- Coordinate the incorporation of any additional technology that poses a threat to the State's sensitive information and critical infrastructure into a cybersecurity plan.

PWDB Policy Compliance

All staff of the PWDB, WSP, TWC, TVC, and other community agencies and partners, must sign the *Prohibited Technologies Agreement* confirming their understanding of the content of this policy. The signed Agreement is required to be included at the time of the submission of the Initial Access Requests and for the Annual Requirements thereafter, as referenced in PWDB Policy 9.1 *Systems Access*. Compliance with this policy will be verified through various methods, including, but not limited to, IT/security system reports and feedback to Management. An employee found to have violated this policy may be subject to disciplinary action, up to and, including prohibition from working in the WSP system and WSP offices, or termination of employment.

PANHANDLE WORKFORCE DEVELOPMENT BOARD
~~Chapter 8 Infrastructure and Internal Controls~~
~~Information Technology (IT) Security, Systems and Computer Access~~
Chapter 10 – Systems and Applications
Section ~~8.5~~ 10.1 **Systems Access** **Effective 5-24-2023**

PURPOSE:
To update Panhandle Workforce Development Board (PWDB) IT Security and Cybersecurity policy **to include information in the Devices and Prohibited Technologies policy, Section 9.1.** Updated information in this policy revision is highlighted in **bold** typeface and in ~~strikethrough~~.

PWDB POLICY:
This policy applies to all Workforce Solutions Panhandle (WSP) staff, Panhandle Regional Planning Commission (PRPC) staff, Texas Workforce Commission (TWC) staff, Texas Veterans Commission (TVC) staff, and other community agencies and partners as noted.

Access to computer systems, equipment, State and local automated systems, and Workforce applications will only be provided to staff who need the information to perform their jobs, and to staff from other agencies or community partners, whose required forms have been received by Board Administrators. WSP and PWDB staff are responsible for protecting Personally Identifiable Information (PII) and other sensitive information from unauthorized disclosure; complying with the requirements of the National Institute of Standards and Technology (NIST) and, as applicable, cybersecurity and information security industry best practices.

It is the policy of TWC to protect the information resources in accordance with the Texas Administrative Code (TAC) Title 1, Part 10, Chapter 202, Subchapter B Information Security Standards and the Information Resources Management Act (Texas Government Code Chapter 2054). TWC will also protect the information resources of the agency in accordance with applicable federal and State Rules and Regulations. Protecting and maintaining the security of agency information resources is a priority. Of particular concern is ensuring the protection of all Texans' sensitive and confidential personal information collected and maintained. At all times, all staff must prioritize data security and take all necessary and appropriate measures to ensure sensitive and confidential information is adequately protected. Staff must protect these assets against unauthorized access, disclosure, modification or destruction, whether accidental or deliberate, as well as assure the availability, integrity, utility, authenticity and confidentiality of information.

As a recipient of Workforce Innovation and Opportunity Act (WIOA) Title I funds, WSP will develop and implement written procedures on the storage and use of disability-related and medical information, as required by TWC Workforce Development (WD) Letter 17-07, as updated. WSP will ensure that the procedures include guidelines for storing information in a manner that provides confidentiality, prohibitions on the use and disclosure of information, except as provided in 29 Code of Federal Regulations (CFR) §38.41(b)(3), and will ensure appropriate staff members are apprised of and comply with all requirements in the WD Letter.

WSP must also record the limited English proficiency and preferred language of each applicant, registrant, participant, and terminated staff, as outlined in WD Letter 17-07, as updated.

Custodians

Custodians are individuals or agents designated as the holder of data and charged with implementing the security controls specified by the owner. Custodians must be knowledgeable with the range of information security risks that need to be managed. Custodians are responsible for:

- Protecting the information in their possession from unauthorized access, alteration, destruction or usage.
- Providing and administering general controls consistent with Information Security policies and standards.
- Establishing, monitoring and operating information systems in a manner consistent with policies and standards issued by the Information Resource Manager (IRM).
- Being knowledgeable with the range of information security risks that need to be managed.
- Reporting all suspicious computer and network security-related activities in accordance with security incident response procedures.
- Assisting owners in understanding and evaluating the cost and effectiveness of security controls and monitoring.

Users

Users are persons who have been authorized to read, enter, or update information and/or to access an information resource in accordance with TWC-defined controls and access Rules. Users include TWC employees, temporary employees, volunteers, interns, private providers of services, WSP staff, and sub-contractors, vendors, auditors, consultants and representatives of other entities or agencies of State government authorized access to TWC Information Resources (IR). Users will be held individually accountable for all actions performed under their User Identification (User ID).

Users have the responsibility to:

- Use the information resource for only the purposes specifically approved by TWC;
- Comply with all security measures, policies and standards defined by TWC and the PWDB, as implemented by WSP, and/or defined by Information Security Officers;
- Use appropriate measures to protect TWC IR equipment or data from unauthorized access or use; and
- Report all suspicious computer and network security-related activities in accordance with security incident response procedures.

Workforce Development Board Administrator Responsibilities

PWDB administrators will determine, assign, and secure Workforce application computer access codes required for WSP staff, PRPC staff, TWC staff, and other community agencies and partners, including changing or resetting users' local passwords, and administering Resource Access Control Facility (RACF) security add(s), change(s), and delete(s) for users.

User Responsibilities

Each agency will ensure that their staff users:

- Are aware of and comply with TWC's data security requirements;

- Understand that under no circumstances are user names, identification codes, passwords, or any other access security codes to be used by anyone other than the user to whom they are assigned and are not to be disclosed to anyone; and
- Understand that they are responsible for any actions completed in Workforce applications under the use of their access security codes.

Each agency will ensure that information obtained from Workforce applications (e.g., participant information) is not republished or redistributed, and ensure that WSP staff protect customers' PII. NIST special publications TWC uses for reference include: NIST SP800-122 Guide to Protecting the Confidentiality of Personally Identifiable Information (PII), at: http://csrc.nist.gov/publications/nistpubs/800-122/sp800-122.pdf.

Account Management

Responsibility for managing access to State automated systems and Workforce applications, (including, but not limited to, those listed below), is as follows:

RACF:

PWDB staff, TVC staff, and WSP staff:
- Board Administrators

TWC staff:
- TWC Program Manager
- TWC Assistant Integrated Service Area (ISA) Manager

WorkInTexas.com:

TWC staff, TVC staff, and WSP staff:
- Workforce Solutions Panhandle WIT Liaison

PWDB staff:
- Board Administrators

TWIST and HHSC:

All PWDB staff and WSP staff:
- Board Administrators

Local network accesses are managed by the PRPC IT Manager and the WSP Systems Administrator.

Access Control

Access privileges should be limited to those necessary for each Staff member's specific job duties. Staff members and other appropriate users will be given access to State and local information systems and Workforce applications only after the required documents are received by Board Administrator(s).

Access requests must be submitted to Board Administrator(s) within 24 hours of identification of the need, and with as much advance notice as possible. WSP will submit all local workforce center staff requests by email to panhandletwist@theprpc.org. All other users will coordinate submission directly with Board Administrator(s).

- **Initial Access Requests**
  The following required forms, including but not limited to, will be provided, to the Board Administrators, in order to grant access:

- **TWC Information Security Agreement, All Employees Form (e P-41).** As per the TWC Agency Board Agreement (ABA), effective 10/1/2022, as updated, the PWDB shall require all persons to whom it grants access to Agency applications, to execute a *P-41 TWC Information Security Agreement, All Employees Form* (e P-41). At a minimum, each user must execute a new e P-41 every two (2) years by the end of the month in which the last P-41 was executed. The e P-41 available at the following web address: P-41 (WF Board Use). The Board Administrator shall maintain a copy of the most recent e P-41 for each user from:
  - All local workforce center staff from WSP, TWC, and TVC; all PWDB staff; appropriate PRPC IT and Finance Division staff; and
  - Single-occurrence users from other community agencies, partners and vendors.

- **Prohibited Technologies Agreement. Texas Governor Greg Abbott has directed all State agencies in Texas, including their employees, contractors, interns, or any users of State-owned networks, to develop a plan providing guidance to ban, and prevent the download, or use, of prohibited technologies; implement network-based restrictions to prevent the use of prohibited technologies; and to prevent prohibited technology-enabled devices from entering or being used in sensitive areas. TWC has issued and updated guidance in Workforce Development (WD) Letter 29-22, as amended, *Ban of TikTok and Other Nonwork-Related Social Network Services*. The PWDB has issued *Devices and Prohibited Technologies* policy requiring a signed Prohibited Technologies Agreement, confirming understanding of the content of this policy, from:**
  - **All local workforce center staff from WSP, TWC, and TVC; and all PWDB staff; and**
  - **Single-occurrence users from other community agencies, partners and vendors.**

- **Form P-48 - Systems Access Report for Other Agencies and Community Partners. As per TWC WD Letter 11-16, a Form P-48 must be completed when providing, terminating, or adjusting access and connectivity permissions to Workforce Applications [e.g., The Workforce Information System of Texas (TWIST) and WorkInTexas.com] that contain personally identifiable information (PII)** from:
  - Single-occurrence users from other community agencies, partners and vendors.

- Certificates of Completion for Computer Based Trainings (CBTs), accessed at: https://www.twc.texas.gov/development/train/board_and_contractor_training_links.html
  - Completed by newly hired local workforce center staff from WSP, TWC, and TVC; all PWDB staff; and appropriate PRPC IT and Finance Division staff, as required in TWC's Agency Board Agreement (ABA), and Workforce Development (WD) Letter 16-08, Change 1, as updated, for:
    (1) Cybersecurity Awareness;
    (2) Fraud Awareness Training; and
    (3) Sensitive Personal Information (SPI) Training.

Staff must print and submit the Certificates of Completion to the appropriate staff within thirty (30) calendar days of accessing TWC systems and electronic resources.

- Completed by single-occurrence users from other community agencies, partners and vendors, as required in TWC's Agency Board Agreement (ABA), for:
  (1) Cybersecurity Awareness; and
  (2) Sensitive Personal Information (SPI) Training.

  Users must print and submit the Certificates of Completion to the appropriate staff, prior to being granted access.

- **Modification to Staff Access**
  WSP will ensure modification of access to increase or decrease privileges necessary for each staff member's specific job duties.

- **Deletion to Access**
  All related accesses must be discontinued within one (1) business day from exit.

  - All local workforce center WSP, TWC, and TVC staff: An initial communication regarding staff exiting from employment will be submitted by email to panhandletwist@theprpc.org, with as much advance notice as possible, followed by applicable original documentation, in the next daily interoffice delivery.
  - All external users from other agencies, community partners, and vendors: An initial communication regarding staff exiting from employment will be submitted by email to panhandletwist@theprpc.org, with as much advance notice as possible, followed by applicable original documentation, including a Form P-48, in the next daily interoffice delivery.

- **Annual Requirements**
  Staff hired in the months of July, August and September, and having completed the Initial Requirements documentation, described on the previous page, are considered in compliance for up to fifteen months until the following October.

  The following will be provided, to the Board Administrators between October 1 and November 10 of each year by all local workforce center staff from WSP, TWC, and TVC; all PWDB staff; appropriate PRPC IT and Finance Division staff:

  - Documentation of current Automation Systems Access for all applicable staff;
  - Form e P-41, from all local workforce center staff from WSP, TWC, and TVC; all PWDB staff; appropriate PRPC IT and Finance Division staff;
  - **Prohibited Technologies Agreement, from WSP, TWC, and TVC; and all PWDB staff;** and
  - Certificates of Completion for Computer Based Trainings (CBTs), accessed at: https://www.twc.texas.gov/development/train/board_and_contractor_training_links.html

    - Completed by all local workforce center staff from WSP, TWC, and TVC; all PWDB staff; and appropriate PRPC IT and Finance Division staff, as required in

TWC's Agency Board Agreement (ABA), and Workforce Development (WD) Letter 16-08, Change 1, as updated, for:

(1) Cybersecurity Awareness;
(2) Fraud Awareness Training; and
(3) Sensitive Personal Information (SPI) Training.

ATTACHMENTS: None.

RESCISSIONS: Chapter 8-Infrastructure and Internal Controls, Section 8.5, Information Technology (IT) Security, Systems and Computer Access, **Effective 12-7-22.**

PANHANDLE
REGIONAL
PLANNING
COMMISSION

ITEM 7

The Cybersecurity Council will be comprised of the Chairperson, Vice Chairperson and, at least one additional member with an interest and/or expertise in IT and cybersecurity-related issues, who are willing to serve on the Cybersecurity Council, and are elected by the Panhandle Workforce Development Board (PWDB) in an Open Public Meeting. At the discretion of the Chairperson, the Council may act on behalf of the PWDB on matters requiring such prompt action that the Board cannot be convened for a special meeting. Such actions will be subject to ratification by the Board.

PANHANDLE WORKFORCE DEVELOPMENT BOARD
CYBERSECURITY COUNCIL

FOR FEBRUARY 22, 2023 – JUNE 30, 2025

PRIVATE SECTOR (AREA I - DALLAM, HARTLEY, MOORE, OLDHAM AND SHERMAN COUNTIES)
Mr. Michael Wright *
Publisher
Moore County News - Press
Dumas, Texas

POST-SECONDARY EDUCATION
Mr. Texas D. "Tex" Buckhaults **
President
Clarendon College
Clarendon, Texas

LABOR ORGANIZATIONS
Mr. Paul Salazar
Training Director, JATC
West Texas Electrical Joint Apprenticeship & Training Committee
Amarillo, Texas

COMMUNITY-BASED ORGANIZATIONS
Ms. Magi York
Executive Director
Panhandle Community Services
Amarillo, Texas

* Denotes the member selected to serve as Chairperson
** Denotes the member selected to serve as Vice Chairperson