PWDB
Cybersecurity Council
Meeting Agenda
January 18, 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, January 18, 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/81526418478?pwd=bForckxnSkJ3bGlOOURJZWpYZDRodz09
(Meeting ID: 815 2641 8478 - Passcode: 857884);

Or may participate by phone (346) 248-7799 (Meeting ID: 815 2641 8478 - Passcode: 857884).

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 May 13, 2022.

4. **CYBERSECURITY COUNCIL MEMBERSHIP FOR 2023-2025**

   Members will be asked to select a new Cybersecurity Council member for the upcoming term.

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.

5. **PANHANDLE WORKFORCE DEVELOPMENT BOARD (PWDB) CYBERSECURITY POLICIES**

Members will be presented with three (3) proposed PWDB Cybersecurity policy updates and one (1) proposed new policy for discussion and input. No action by the Council will be taken in the closed session.

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

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

6. **VOTE ON PWDA CYBERSECURITY POLICIES**

Members will be asked to vote on the three (3) proposed PWDB Cybersecurity policy updates and one (1) proposed new policy described in the previous item. The results of the discussion, input and subsequent vote will be reported to the full PWDB at its February 22, 2023 meeting.

7. **OPEN DISCUSSION**

Members have the opportunity to discuss topics of interest. 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 12th day of January 2023, at 415 Southwest Eighth Avenue, Amarillo, Texas, at 11:00 a.m.

Leslie Hardin

Leslie Hardin

AN EQUAL OPPORTUNITY EMPLOYER / PROGRAM
Auxiliary aids and services are available upon request to individuals with disabilities / Relay Texas: 711

PANHANDLE
REGIONAL
PLANNING
COMMISSION

ITEM 3

PANHANDLE REGIONAL PLANNING COMMISSION

PANHANDLE WORKFORCE DEVELOPMENT BOARD

Cybersecurity Council

Minutes

May 13, 2022

A meeting of the Panhandle Workforce Development Board's Cybersecurity Council was held at 11:45 a.m. on Friday, May 13, 2022. 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.

Ms. Magi York, presided.

COUNCIL MEMBERS PRESENT:

- Michael Wright, Moore County News - Press
- Magi York, Panhandle Community Services

COUNCIL MEMBER ABSENT:

- Texas "Tex" Buckhaults, Clarendon College

STAFF CYBERSECURITY COMMITTEE PRESENT:

Kathy Cabezuela, Leslie Hardin, Marin Rivas, and Samantha Roybal, Panhandle Regional Planning Commission (PRPC); Trent Morris and Anthony Solis, Workforce Solutions Panhandle (WSP).

OTHERS PRESENT:

Dennis Garvey, Panhandle Community Services.

1. CALL TO ORDER

   Ms. York 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 November 15, 2021 meeting. Mr. Wright moved to approve the minutes as presented. Ms. York seconded the motion; the motion carried.

4. CURRENT CYBERSECURITY COUNCIL MEMBERSHIP LIST

Panhandle Workforce Development Board members serving on the Panhandle Workforce Development Board's Cybersecurity Council: Mr. "Tex" Buckhaults, Mr. Michael Wright, and Ms. Magi York. This item was for informational purposes only.

5. CYBERSECURITY COUNCIL MEMBERSHIP FOR 2022-2023

Members volunteered to serve an additional term on the Council. Ms. York moved to continue the current membership for another term. Mr. Wright seconded the motion; the motion carried.

6. CYBERSECURITY COUNCIL BYLAWS

Members were asked to consider amendments to the set of bylaws governing the Council:

- In the meeting agenda item, staff had requested that the Cybersecurity Committee membership be reduced from "at least two (2) WSP staff" to "at least one (1) WSP staff"; and
- During the meeting, Mr. Wright suggested the next Cybersecurity Council membership term be extended from one year to three years.

Mr. Wright moved to amend the bylaws with both changes, and forward them to the Panhandle Workforce Development Board Chair for signature. Ms. York seconded; the motion carried.

** AT THIS POINT IN THE MEETING, MEMBERS ENTERED 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.

7. PANHANDLE WORKFORCE DEVELOPMENT BOARD (PWDB) CYBERSECURITY POLICIES

Members were presented with seven (7) proposed PWDB Cybersecurity policies for discussion and input. No action by the Council was taken in the closed session.

a) Information Security
b) Acceptable Use of Information Technology Resources
c) Incident Response
d) Information Logging Standard
e) Secure Configuration
f) Account Management / Access Control Standard
g) Virtual Private Network

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

8. VOTE ON PWDB CYBERSECURITY POLICIES

Members were asked to vote on the seven (7) PWDA Cybersecurity Policies described in the previous item. The motions were as follows:

a) Information Security - Ms. York moved to accept the policy, with two edits. Mr. Wright seconded the motion; the motion carried.
b) Acceptable Use of Information Technology Resources - Ms. York moved to accept the policy. Mr. Wright seconded the motion; the motion carried.
c) Incident Response - Ms. York moved to accept the policy. Mr. Wright seconded the motion; the motion carried.
d) Information Logging Standard - Ms. York moved to accept the policy. Mr. Wright seconded the motion; the motion carried.
e) Secure Configuration - Ms. York moved to accept the policy. Mr. Wright seconded the motion; the motion carried.
f) Account Management / Access Control Standard - Ms. York moved to accept the policy. Mr. Wright seconded the motion; the motion carried.
g) Virtual Private Network - Ms. York moved to accept the policy. Mr. Wright seconded the motion; the motion carried.

Mr. Wright made a motion to accept the policies, with the two edits, and for them to be presented to the PWDB at its May 25, 2022 meeting. Ms. York seconded the motion; the motion carried.

9. OPEN DISCUSSION

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

10. FINAL PUBLIC COMMENT PERIOD

None.

11. ADJOURN

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

PANHANDLE
REGIONAL
PLANNING
COMMISSION

ITEM 4

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

PANHANDLE
REGIONAL
PLANNING
COMMISSION

ITEM 5(a)

ACCEPTABLE USE OF INFORMATION TECHNOLOGY RESOURCES
Area 1 - Identify **Policy 1.3 - *Update*** **Effective 02-22-2023**

Purpose

Appropriate organizational use of information and Information Technology (IT) resources, and effective security of those resources, require the participation and support of the organization's workforce ("users"). Inappropriate use exposes the organization to potential risks including virus attacks, compromise of network systems and services, and legal issues.

Authority

The computers used by staff and customers of the Panhandle Workforce Development Board's (PWDB) Workforce Solutions Panhandle (WSP) offices are the property of the Panhandle Regional Planning Commission (PRPC) and the Texas Workforce Commission (TWC). Those using a computer and/or having access to the network must follow the guidelines outlined in this document.

Information Statement

Except for any privilege or confidentiality recognized by law, individuals have no legitimate expectation of privacy during any use of the organization's IT resources or in any data on those resources. Any use may be monitored, intercepted, recorded, read, copied, accessed or captured in any manner including in real time, and used or disclosed in any manner, by authorized personnel without additional prior notice to individuals. Periodic monitoring will be conducted of systems used, including but not limited to: all computer files; and all forms of electronic communication (including email, text messaging, instant messaging, telephones, computer systems and other electronic records). In addition to the notice provided in this policy, users may also be notified with a warning banner text at system entry points where users initially sign on about being monitored and may be reminded that unauthorized use of the WSP's IT resources is not permissible.

WSP may impose restrictions, at the discretion of their executive management, on the use of a particular IT resource. WSP may block access to certain websites or services not serving legitimate business purposes or may restrict user ability to attach devices to WSP's IT resources (e.g., personal USB drives, iPods). Users accessing applications and IT resources through personal devices must only do so with prior approval or authorization from the Cybersecurity/Systems Administrator.

Acceptable Use

All uses of information and information technology resources must comply with all policies, standards, procedures, and guidelines, as well as any applicable license agreements and laws including federal, State, local and intellectual property laws. Consistent with the foregoing, the acceptable use of information and IT resources encompasses the following duties:

- Understanding the baseline information security controls necessary to protect the confidentiality, integrity, and availability of information;
- Protecting information and resources from unauthorized use or disclosure;
- Protecting personal, private, sensitive, or confidential information from unauthorized use or disclosure;

- **Using a Virtual Private Network (VPN) when remotely accessing WSP network resources;**
- Observing authorized levels of access and utilizing only approved IT technology devices or services; and
- Immediately reporting suspected information security incidents or weaknesses to the appropriate manager and the Cybersecurity/Systems Administrator.

Unacceptable Use

The following list is not intended to be exhaustive, but is an attempt to provide a framework for activities that constitute unacceptable use. Users, however, may be exempted from one or more of these restrictions during their authorized job responsibilities, after approval from the Cybersecurity/Systems Administrator. Unacceptable use includes, but is not limited to, the following:

- Unauthorized use or disclosure of personal, private, sensitive, and/or confidential information;
- Unauthorized use or disclosure of WSP information and resources;
- Distributing, transmitting, posting, or storing any electronic communications, material or correspondence that is threatening, obscene, harassing, pornographic, offensive, defamatory, discriminatory, inflammatory, illegal, or intentionally false or inaccurate;
- Attempting to represent WSP in matters unrelated to official authorized job duties or responsibilities;
- Connecting unapproved devices **(i.e. Cell Phones, iPads)** to the network or any IT resource;
- Connecting WSP IT resources to unauthorized networks;
- Connecting to any wireless network while physically connected to the wired network;
- Installing, downloading, or running software that has not been approved following appropriate security, legal, and/or IT review in accordance with policies;
- Connecting to commercial email systems (e.g., Gmail, Hotmail, Yahoo) without prior management approval (WSP must recognize the inherent risk in using commercial email services as email is often used to distribute malware);
- **Unauthorized use of Removable Media (i.e. USB Storage device) for storage of WSP information;**
- Using an WSP IT resources to circulate unauthorized solicitations or advertisements for non-work-related purposes including religious, political, or not-for-profit entities;
- Providing unauthorized third parties, including family and friends, access to IT information, resources or facilities;
- Using organization IT information or resources for commercial or personal purposes, in support of "for-profit" activities or in support of other outside employment or business activity (e.g., consulting for pay, business transactions);
- Propagating chain letters, fraudulent mass mailings, spam, or other types of undesirable and unwanted email content using IT resources; and
- Tampering, disengaging, or otherwise circumventing WSP or third-party IT security controls.

Occasional and Incidental Personal Use

Occasional, incidental and necessary personal use of IT resources is permitted, provided such use: is otherwise consistent with this policy; is limited in amount and duration; and does not impede the ability of the individual or other users to fulfill WSP's responsibilities and duties, including

but not limited to, extensive bandwidth, resource, or storage utilization. Exercising good judgment regarding occasional and incidental personal use is important. The Cybersecurity/Systems Administrator may revoke or limit this privilege at any time.

Individual Accountability

Individual accountability is required when accessing all IT resources and WSP information. Staff is responsible for protecting against unauthorized activities performed under their user ID. This includes locking your computer screen when you walk away from your system, and protecting your credentials (e.g., passwords, tokens or similar technology) from unauthorized disclosure, **and securing Personal Identifying Information (PII) when leaving your workspace**. Credentials must be treated as confidential information, and must not be disclosed or shared**. If the security of a password is in doubt, the password should be changed immediately. In addition, staff should not connect personally owned mobile devices to the WSP Wi-Fi. If using a mobile device to connect to communication tools (i.e. Email, Teams), that device should have a Personal Identification Number (PIN) or other authentication mechanism enabled. Additionally, guests and staff can connect to the WSP "Guest" Wi-Fi.**

Restrictions on Off-Site Transmission and Storage of Information

Users must not transmit restricted, non-public, personal, private, sensitive, or confidential information to or from personal email accounts (e.g., Gmail, Hotmail, Yahoo) or use a personal email account to conduct business unless explicitly authorized. Users must not store restricted, non-public, personal, private, sensitive, or confidential information on a non-organizational issued device, or with a third-party file storage service that has not been approved for such storage by the Cybersecurity/Systems Administrator. Devices that contain WSP information must be attended at all times or physically secured and must not be checked in transportation carrier luggage systems.

User Responsibility for IT Equipment

Users are routinely assigned or given access to IT equipment in connection with their official duties. This equipment belongs to WSP and must be immediately returned upon request or at the time an employee is separated from the organization. Users may be financially responsible for the value of equipment assigned to their care if it is not returned to WSP. Should IT equipment be lost, stolen or destroyed, users are required to provide a written report of the circumstances surrounding the incident. Users may be subject to disciplinary action which may include repayment of the replacement value of the equipment. WSP has the discretion to not issue or re-issue IT devices and equipment to users who repeatedly lose or damage IT equipment.

Use of Social Media

The use of public social media sites to promote organizational activities requires written pre-approval. Approval is at the discretion of appropriate management and the Cybersecurity/Systems Administrator. Approval may be granted upon demonstration of a business need, and a review and approval of service agreement terms. Final approval by appropriate management should define the scope of the approved activity, including, but not limited to, identifying approved users.

Unless specifically authorized, the use of WSP email addresses on public social media sites is prohibited. In instances where users access social media sites on their own time utilizing personal resources, they must remain sensitive to expectations that they will conduct themselves in a responsible, professional, and secure manner with regard to references to WSP and staff. These expectations are outlined below.

a. Use of Social Media within the Scope of Official Duties

Appropriate management, must review and approve the content of any posting of public information, such as blog comments, tweets, video files, or streams, to social media sites on behalf of WSP. However, approval is not required for postings to public forums for technical support, if participation in such forums is within the scope of the user's official duties, has been previously approved by his or her supervisor, and does not include the posting of any sensitive information, including specifics of the IT infrastructure. In addition, approval is not required for postings to private, WSP approved social media collaboration sites. Blanket approvals may be granted, as appropriate.

Accounts used to manage WSP's social media presence are privileged accounts and must be treated as such. These accounts are for official use only and must not be used for personal use. Passwords of privileged accounts must follow information security standards, be unique on each site, and must not be the same as passwords used to access other IT resources.

b. Guidelines for Personal Use of Social Media

Staff should be sensitive to the fact that information posted on social media sites clearly reflects on the individual and may also reflect on the individual's professional life. Consequently, staff should use discretion when posting information on these sites and be conscious of the potential perceptions of and responses to the information. It is important to remember that once information is posted on a social media site, it can be captured and used in ways not originally intended. It is nearly impossible to retract, as it often lives on in copies, archives, backups, and memory cache.

Users should respect the privacy of WSP's staff and not post any identifying information of any staff without permission (including, but not limited to, names, addresses, photos, videos, email addresses, and phone numbers). Users may be held liable for comments posted on social media sites.

If a personal email, posting, or other electronic message could be construed to be an official communication, a disclaimer is strongly recommended. A disclaimer might be: "The views and opinions expressed are those of the author and do not necessarily reflect those of the organization."

Users should not use their personal social media accounts for official business, unless specifically authorized. Users are strongly discouraged from using the same passwords in their personal use of social media sites as those used on organizational devices and IT resources, to prevent unauthorized access to resources if the password is compromised.

History - This standard shall be subject to periodic review to ensure relevancy.

Date	Description
5/13/2022	Cybersecurity Council Approval of Initial Document.
5/25/2022	Panhandle Workforce Development Board Approval of Cybersecurity Council Document.
5/26/2022	Panhandle Workforce Development Consortium's Governing Body Concurrence with Panhandle Workforce Development Board's Approval of Document.

PANHANDLE
REGIONAL
PLANNING
COMMISSION

ITEM 5(b)

SECURE CONFIGURATION		
Area 2 - Protect	**Policy 2.1 - *Update***	**Effective 02-22-2023**

Purpose

To establish baseline configurations for information systems that are owned and/or operated by the Panhandle Workforce Development Board. Effective implementation of this policy will maximize security and minimize the potential risk of unauthorized access to information and technology.

Scope

Standard secure configuration profiles must be used in addition to the latest vendor security guidance. Alterations to profiles must be based on policy, standard, or procedure compliance, or to fulfill a business need. Alterations to profiles must be approved by the Cybersecurity/System Administrator.

The initial setup, software installation, and security configuration of new systems must be performed in a secure physical environment.

Changes to configurations must be formally identified, proposed, reviewed, analyzed for security impact, tested, and approved by the Cybersecurity/System Administrator prior to implementation.

The Cybersecurity/System Administrator must maintain configuration management plans that define detailed processes and procedures for how configuration management is used to support secure system development life cycle activities at the information system level.

Secure Configuration

1. For security, compliance and maintenance purposes, service accounts are prohibited. Only authorized personnel can log in, monitor systems, process and network traffic.
2. Operating System configuration should be in accordance with Secure Configuration Policy for:
   - Servers, Windows Server 2016, 2019, Linux Ubuntu 20.04
   - Workstations, Windows 10, 21H2 baseline; and
   - Laptops, Windows 10 20H1 baseline
3. Through Group Policy all Windows servers, workstations, and laptops will operate with a High Security Baseline in line with DOD/Microsoft Secure baseline requirements.
4. All workstations and laptops deployed must have their hardware, operating system and asset tag information logged and documented.
5. Services and applications that will not be used must be disabled.
6. Access to services must be logged and protected through access-control methods.
7. Most recent relevant security patches must be installed on the system within one week of being approved, the only exception being when immediate application would interfere with business requirements.
8. Always use standard security principals of least required access to perform a function. Do not use root or domain admin credentials when a non-privileged account is sufficient.
9. The latest version of Endpoint software must be installed and configured for automatic updates and scans.

Server Configuration

1. All internal servers deployed must be documented with the following information:
   - Hardware and Operating system version; and
   - Main Functions and Applications
2. When administering remotely, SSH must be used for Linux servers and RDP with Multi-factor authentication must be used for Windows servers. For security, compliance and maintenance purposes, end user and service accounts are prohibited.
3. Servers should be located in an access-controlled environment (Server rooms, locked in secure server cabinet)
4. All security-related events on critical and sensitive systems must be logged and audit trails must be saved as follows:
   - All security related logs must be kept online for 30 days.
   - Daily incremental backups must be retained for 30 days.
   - Weekly full backups must be retained for 180 days.
   - Monthly full backups must be retained for 360 days.
5. Security related events must be reported to the Cybersecurity Committee. Corrective measures will be recommended for implementation as needed.
6. All servers are configured to not be used to browse the internet.

Workstation Configuration

Local Administrative rights will be granted as needed.

Laptop Configuration

1. Local Administrative rights will not be granted for laptops.
2. Barracuda VPN gateway is installed by default, if VPN access is needed the corresponding profile will be installed by the Cybersecurity/System Administrator.

Incident Response

1. In event of security-related event corrective measures will be taken in accordance with the Incident Response Policy.

2. Security-related events include, but are not limited to:

- **Port-Scan Attacks.**
- **Evidence of unauthorized access to privileged accounts.**
- **Loss of Data Integrity.**
- **Anomalous occurrences that are not related to specific applications on the host.**

History - This standard shall be subject to periodic review to ensure relevancy.

Date	Description
5/13/2022	Cybersecurity Council Approval of Initial Document.
5/25/2022	Panhandle Workforce Development Board Approval of Cybersecurity Council Document.
5/26/2022	Panhandle Workforce Development Consortium's Governing Body Concurrence with Panhandle Workforce Development Board's Approval of Document.

PANHANDLE
REGIONAL
PLANNING
COMMISSION

ITEM 5(c)

~~INCIDENT RESPONSE~~ RISK ASSESSMENT AND MITIGATION		
Area 3 - Detect	**Policy 3.1 - *Update***	**Effective 02-22-2023**

Purpose of Policy

To ensure that the Cybersecurity/Systems Administrator performs ~~Incident Response~~ **Risk Assessment and Mitigation** that is in compliance with IT security policies, standards, and procedures.

Penetration Testing

The Cybersecurity/Systems Administrator will:

- Test the incident response capability for the Information Systems using a third-party company for external penetration testing.
- Coordinate the incident response/penetration testing with Workforce Solutions Panhandle (WSP) and Panhandle Workforce Development Board (PWDB) management responsible for related plans such as Business Continuity, Disaster Recovery Plans and Contingency Plans.
- Disseminate results of penetration testing to the PWDB Cybersecurity Committee.
- Document Penetration Test results in annual report.
- The PWDB Cybersecurity Committee will provide reports and recommended actions to the PWDB Cybersecurity Council.

Risk Assessment

The Cybersecurity/Systems Administrator will:

- Conduct an assessment of risk, including the likelihood and magnitude of harm, from the unauthorized access, use, disclosure, disruption, modification, or destruction of the information system and the information it processes, stores, or transmits.
- Document risk assessment results in annual IT Risk Assessment.
- Disseminate risk assessment results to PWDB Cybersecurity Committee.
- Update the risk assessment whenever there are significant changes to the information system or environment of operation (including the identification of new threats and vulnerabilities), or other conditions that may impact the security state of the system.

Vulnerability Scanning

The Cybersecurity/Systems Administrator will:

- Scan for surface vulnerabilities in the information system and hosted applications daily and immediately when new vulnerabilities potentially affecting the system/applications are identified and reported.
- Deep-scan for infrastructure vulnerabilities in the information system and hosted applications weekly and immediately when new vulnerabilities potentially affecting the system/applications are identified and reported.
- Employ vulnerability scanning tools and techniques that facilitate interoperability among tools and automate parts of the vulnerability management process by using standards for:
  i. Enumerating platforms, software flaws, and improper configurations.
  ii. Formatting checklists and test procedures.
  iii. Measuring vulnerability impact.
- Analyze vulnerability scan reports and results from security control assessments.

- Remediate legitimate vulnerabilities within one month in accordance with an organizational assessment of risk.
- Utilize information obtained from the vulnerability scanning process and security control assessments to help eliminate similar vulnerabilities in other information systems (i.e., systemic weaknesses or deficiencies).
- Employ vulnerability scanning tools that include the capability to readily update the information system vulnerabilities to be scanned.

Incident Response Testing and Monitoring

The Cybersecurity/Systems Administrator will:

- Test the Incident Response Capability protocols with software to determine response effectiveness.
- Coordinate incident response testing results with PWDB Cybersecurity Committee for plans on Business Continuity, Contingency and Disaster Recovery.

~~**Incident Handling**~~

~~The Cybersecurity/Systems Administrator will ensure that:~~

- ~~Security Threats detected by Endpoint Detection software will be quarantined immediately.~~
- ~~Security Threats detected by Vulnerability Scanning will be patched or removed from the network within 30 days of detection.~~
- ~~Security Threats detected by Penetration Testing must be patched within 30 days of results.~~

~~The Cybersecurity/Systems Administrator will:~~

- ~~Coordinate incident handling results with Cybersecurity Committee for plans on Business Continuity, Contingency and Disaster Recovery.~~
- ~~Incorporate lessons learned from ongoing incident handling activities into incident response procedure and implement the resulting changes.~~

History - This standard shall be subject to periodic review to ensure relevancy.

Date	Description
5/13/2022	Cybersecurity Council Approval of Initial Document.
5/25/2022	Panhandle Workforce Development Board Approval of Cybersecurity Council Document.
5/26/2022	Panhandle Workforce Development Consortium's Governing Body Concurrence with Panhandle Workforce Development Board's Approval of Document.

PANHANDLE
REGIONAL
PLANNING
COMMISSION

ITEM 5(d)

INCIDENT RESPONSE		
Area 4 - Respond	**Policy 4.1**	**Effective 02-22-2023**

Purpose

To establish the incident response process. This policy will define to whom it applies and under what circumstances, and it will include the definition of a cybersecurity incident, staff roles and responsibilities, standards and metrics (e.g., to enable prioritization of the incidents), as well as reporting, remediation, and feedback mechanisms, as described in Attachment A, Cybersecurity Incident Response Plan and Privacy Incident Response Plan, as required by the Texas Workforce Commission (TWC) Agency Board Agreement (ABA), as amended.

The Panhandle Workforce Development Board (PWDB) and Workforce Solutions Panhandle (WSP) Information Security's intentions for a Cybersecurity Incident Response policy are to focus significant attention on Cybersecurity and how WSP's established culture of openness, trust and integrity should respond to such activity. WSP Information Security is committed to protecting WSP's employees, customers and partners from illegal or damaging actions by individuals, either knowingly or unknowingly.

Background

This policy mandates that any individual who suspects that a theft, breach or exposure of WSP Protected data or WSP Sensitive data has occurred must immediately provide a description of what occurred to the Cybersecurity/Systems Administrator, who will investigate all reported Cybersecurity Incidents to confirm if a Cybersecurity Incident has occurred. If a Cybersecurity Incident has occurred, the Cybersecurity/Systems Administrator will follow the appropriate procedure in place.

Scope

This policy applies to all whom collect, access, maintain, distribute, process, protect, store, use, transmit, dispose of, or otherwise handle Personally Identifiable Information (PII) or Protected Health Information (PHI) of WSP staff and customers.

ATTACHMENT:

Attachment A - Cybersecurity Incident Response Plan and Privacy Incident Response Plan

ATTACHMENT A
Cybersecurity Incident Response Plan and Privacy Incident Response Plan

Confirmed Incident for Protected or Sensitive Data

As soon as a theft, data breach, exposure, or Cybersecurity incident occurs, the process of removing all access to that resource will begin. The Cybersecurity/Systems Administrator will physically segregate and power off affected resources as applicable and will notify the WSP Director. The WSP Director will notify the Workforce Development Director and collectively they will determine who else will be informed and what actions will be taken in accordance with the TWC ABA and PWDB Cybersecurity Policy 1.4 Information Logging Standard.

TWC Security Management

In the event of a security violation, or if a breach is detected, or if the PWDB or WSP has any reason to suspect that the security or integrity of data has been or might be compromised in any way, the Workforce Development Director shall:

1) Notify, in the case of:
   - A Cybersecurity Incident Response - TWC's Chief Information Security Officer within twenty-four (24) hours via email to CISO@twc.texas.gov; and/or
   - A Privacy Incident Response - Within twenty-four (24) hours via email to: IncidentReports.RSM@twc.state.tx.us;
2) Comply with the notification requirements in Section 521.053, *Business & Commerce Code, Notification Required Following Breach of Security of Computerized Data*, which states that "disclosure shall be made without unreasonable delay and in each case not later than the 60th day after the date on which the person determines that the breach occurred, except … at the request of a law enforcement agency that determines that the notification will impede a criminal investigation … or as necessary to determine the scope of the breach and restore the reasonable integrity of the data system"; and
3) Comply with TWC directives in resolving any incidents.

Cyber Insurance

The PWDB, through WSP, will maintain Cyber Insurance with coverage including, but not limited to, Contingent and Direct System Failure, Business Interruption, and Cyber Extortion. Following detection of a theft, data breach, exposure, or Cybersecurity incident, the WSP Director will notify the Insurance Provider according to the instructions prescribed in the current policy. Should the WSP Director be unavailable, the Workforce Development Director and/or the Cybersecurity/Systems Administrator will notify the Insurance Provider according to the policy's instructions.

WSP will provide access to forensic investigators and experts to determine how the breach or exposure occurred; the types of data involved; the number of internal/external individuals and/or organizations impacted; and analyze the breach or exposure to determine the root cause, as needed.

Develop a Communication Plan

The WSP Director and the Workforce Development Director will determine how to communicate the breach to: a) internal employees, b) the public, and c) those directly affected.

Incident Handling

The Cybersecurity/Systems Administrator will ensure that:

- Security Threats detected by Endpoint Detection software will be quarantined immediately;
- Security Threats detected by Vulnerability Scanning will be patched or removed from the network within 30 days of detection; and.
- Security Threats detected by Penetration Testing must be patched within 30 days of results.

The Cybersecurity/Systems Administrator will:

- Coordinate incident handling results with the PWDB Cybersecurity Committee for plans on Business Continuity, Contingency and Disaster Recovery; and
- Incorporate lessons learned from ongoing incident handling activities into incident response procedure and implement the resulting changes.