WORKFORCE SOLUTIONS
of the Coastal Bend

POLICY

CATEGORY:	**Information Technology & Data Management**	**No: 7.0.101.02**
TITLE:	**Computer & Personally Identifiable Information Access & Security**	
SUPERSEDES:	**7.0.101.02, dtd July 16, 2015**	
EFFECTIVE:	**September 28, 2018**	
BOARD APPROVAL:	**September 27, 2018**	
REVIEW DATE:	**September 13, 2018**	

I. PURPOSE:

To establish access criteria for contracted service providers and the public to the Coastal Bend Workforce Development Board ("Board") and/or Texas Workforce Commission (TWC) Information Systems.

II. DEFINITIONS:

Board – The Coastal Bend Workforce Development Board, operating as Workforce Solutions of the Coastal Bend.

Service Providers – A business entity or person, except a state agency, who contracts with the Board to provide workforce services, including One-Stop services.

Approved User – An individual who is *authorized* by the Board's Network Administrator to utilize and access the computer and/or information system bought or maintained by the Board.

Public – Individuals who are not approved users are deemed *unauthorized* by the Board's Network Administrator to connect to, utilize and access the information systems maintained by the Board, regardless of affiliation.

III. POLICY STATEMENT:

TWC grants the Board access to its information systems to enable its staff and service provider staff the resources to accomplish their assigned duties. The security of the data stored including physical security is critical and as a result the Board has zero tolerance for any and all violations.

Only approved users who have written authorization to access the Board's and TWC's computers and the information system are entitled to use and/or access the equipment and network services. Approved users are required to safeguard their computer passwords and customer files to ensure against unauthorized use. Members of the public are not allowed to connect, use or access the system regardless of affiliation. Permitting members of the public to connect to Board and/or TWC computers and network systems is prohibited and in violation of this policy. Failure by approved users to strictly comply with this policy will result in the immediate revocation of access privileges and may be subject to prosecution under one or more applicable statutes.

All information, whether written, or in electronic format, is the property of the Board and is subject to the Public Information Act. To secure all data, approved users are prohibited from deleting any files or information from the Board's computers. Any intentional violations are subject to prosecution and fines under Section 552.351 of the Act. Although retention schedules vary, the Board's retention of records will be in accordance to the Texas State Library and Archives Commission (TSLAC).

IV. PROCEDURES:

To grant authorization, all prospective users must complete the forms listed below. The authorization is subject to the approval of the Network Administrator. The approved user granted authorization is responsible for reading and understanding this policy and the related forms.

The following information is provided as an illustration of prohibited uses and responsibilities and is not intended to address all situations. All questions may be referred to the Network Administrator.

A. Computer Use

Computers cannot be used for transmitting, retrieving, receipt or storing of any communication that is illegal or contrary to Board policy or business interests or that could cause the appearance of such.

Approved users are prohibited from engaging in, attempting to engage in or assisting others in:

- Sharing personal or confidential information of customers;
- Permitting the public to connect to, use or access the computers and information systems.
- Monitoring or intercepting the files or electronic communications of other employees or third parties;
- Hacking or obtaining access to systems or accounts without authorization to use;
- Making or attempting to make any deliberate, unauthorized change to data on an Information Technology (IT) system;
- Using or permitting others to log-in with approved user's password; and
- Breaching, testing or monitoring computer or network security systems.

B. Passwords

Approved users are prohibited from allowing any member of the public or any other approved user from using their Board issued password. Passwords must be used **only** by the approved user. Approved users are strictly responsible for the protection and use of their passwords. Failure to strictly comply with this policy will result in the immediate revocation of access privileges and may be punishable as a criminal offense under Chapter 33 of the Texas Penal Code.

Passwords are assigned to approved users at the request of a direct supervisor and with the approval of the Center Manager. Logon or system passwords must be used on computers situated in areas frequented by the public.

Passwords must meet the following guidelines:

a. Not easily discernible and must contain numbers and letters.
b. At least one lowercase and one uppercase letter.
c. At least 8 characters in length.
d. Cannot be reused.
e. Kept in a secured location.

C. Software

Downloading of any unauthorized software is strictly prohibited. This includes all freeware, shareware, toolbars, screensavers, hardware, I-tunes or internet utilities, etc. Only software downloaded and installed by the Board's I.T. personnel is approved for use.

All Board computer property is subject to unannounced review. Any software, media, etc. that has been installed without approval, is in violation of this policy and will be removed.

D. Personal Use

The computers, electronic media and services made available by the Board are provided to assist approved users in the performance of their jobs. Use of electronic media (sending or receiving) for personal, non-business purposes during non-working hours is not allowed. However, all personal use must comply with this policy. Streaming video and/or audio is NOT allowed.

E. Physical Security

Minimum protection standards (MPS) establish a uniform method and minimum standards of physically protecting data and systems that require safeguarding. These standards must be applied. Because local factors might require additional security measures, management must analyze local circumstances to determine space, container, and other physical security needs.

MPS require two barriers for the protection of PII under normal operating conditions.
Some examples of barriers are:

- Staff presence
- Locked office, locked file cabinet, or another lockable container
- Access control system such as a card reader
- Restricted access by means of keypad entry or secondary-level card key access
- Out of plain sight; as a second barrier only

F. Review & Monitoring of Usage

The Board reserves the right to review and monitor usage to detect inappropriate or illegal use which may be in violation of Board or TWC policies and agreements.

The Board reserves the right to review all electronic files and messages to the extent necessary to ensure electronic media and services are used in compliance with the law, this policy and other Board policies.

Approved users should note that electronic communications are not private and remain the property of the Board and/or TWC.

V. RELATED POLICY INFORMATION:

WD Letter 11-16, Access and Data Security for Workforce Applications, dtd June 15, 2016
WD Letter 02-18, Handling and Protection of Personally Identifiable Information and Other Sensitive Information, dtd March 23, 2018

VI. RESPONSIBILITIES:

President/CEO – Responsible for the Board's adherence to this policy.
Information Technology Department - Responsible for reviewing and granting authorization and monitoring compliance to this policy.
Service Providers Staff – Responsible for coordinating the Board's compliance and communicating this policy to staff.

VII. FORMS AND INSTRUCTIONS:

Form P-41 – TWC Information System Security agreement for Board Users and Other Users.
Security and Privacy Agreements as required by TWC and the Board
Request for User Access to Health and Human Services Commission (HHSC) Systems

VIII. DISTRIBUTION:

☐ Board of Directors ☒ Board Staff ☒ Service Provider Staff

IX. SIGNATURES:

Harry Peterson — **Reviewed by EO Officer**

10/4/18 — **Date**

President/CEO

10/4/18 — **Date**