HEART OF TEXAS WORKFORCE DEVELOPMENT BOARD, INC.
PROPOSED POLICY

ID NO.:	HWD 008-10	**DATE ISSUED:**	August 19, 2010
PROGRAM:	All	**KEYWORD:**	Automation

Subject: Definition, acceptable use and limits on computer data, hardware, and software.

Purpose: Workforce Solutions Heart of Texas Workforce information resources are assets that must be protected from unauthorized disclosure, modification, use, or destruction. Appropriate steps must be taken to ensure that its integrity, confidentiality, and availability are not compromised.

References: Texas Workforce Commission Enterprise Information Security Standards and Guidelines and Texas Workforce Commission Information Technology User Reference guide

Discussion: Workforce Solutions Heart of Texas Workforce follows guidance prescribed by the Texas Workforce Commission for information technology and security.

This policy is crafted to not only provide general and specific guidelines but to increase the awareness of users to the potential risks associated with information technology.

Policy:

All users shall comply with the policies, standards, guidelines, and procedures as set forth in this policy.

1. The basis for this policy is the TWC Enterprise Security Policy. A copy has been attached to this policy.
2. Use of the TWC Information Technology User Reference guide where applies to local Boards
3. In addition to the standards and guidelines outlines in the TWC Enterprise Security Policy the Board has implemented the following
    - Password Requirements
        - User passwords must be at least 8 letters and numbers
        - Requirement of changing passwords every 60 days (with a 14 day notification) for WIT and individual workstation desktops

- After three (3) failed attempts the user will be lockout and must notify IT staff for a reset

- Security Controls
  - Terminated staff accounts will be removed from the server after 60 days without a written request from upper management.
  - A written request, to include reason for access, from upper management must be submitted to IT staff for a supervisor to gain temporary access to another's staff member's account.
  - Customer information such as names and social security numbers will not be transmitted via instant messaging
  - Customer information containing social security numbers must not be transmitted via e-mail unless the information is password protected.
  - Client information on copiers or printers in unsecure areas must be retrieved immediately.
  - Only authorized **staff** has access to customer files, Smart files, TWIST or other sensitive information. Temporary workers must be supervised at all times when working with customer information
  - Breaches in information security must be reported to upper management and the Board immediately
  - Client Information placed on disks, drives, etc must be password protected and kept secure at all times
  - Laptops and desktops must be secure at all times, password protected, and set to time out and lock at a prescribed time if not in use.
  - All computers will be powered down and turned off at the end of the workday, during lunch hours,or when away from the desk for any extended period of time.

Public Review and Comment: The public is invited to submit comments on this proposed policy. Please submit comments in writing to Aquanetta Brobston at 801 Washington Ave, Suite 700, Waco, TX 76701 or aquanetta.brobston@hotworkforce.com by noon on July 9, 2010.

Effective Date: August 19, 2010