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

HEART OF TEXAS WORKFORCE DEVELOPMENT BOARD, INC.

POLICY

ID NO.: HWD CS 011-23	**DATE ISSUED:** 3/1/2023
PROGRAM: Cybersecurity	**KEYWORD:** System & Information Integrity Policy

SUBJECT: System & Information Integrity Policy

PURPOSE: To provide staff with information and guidance on the System & Information Integrity expectations and oversight within the Heart of Texas Workforce Solutions environment.

REFERENCES: TWC Information Security Manual 2.0(5) Section 3.1.4

POLICY: SYSTEM AND INFORMATION INTEGRITY POLICY

GENERAL POLICY

The Heart of Texas Workforce Development Board (HOTWDB) Information Technology Security Steering Committee (ITSSC) has developed, documented, and disseminated an audit and accountability policy and procedure that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance.

The HOTWDB ITSSC will develop, document, and disseminate a system and information integrity policy and procedures that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance to defined groups and roles.

The HOTWDB ITSSC will review the system and information integrity policy and procedures no less than annually.

GROUPS	ROLES	PERSONNEL
Domain Admins	Administrator	IT Staff, Twist Update, PRTG, WFS Backup, Postmaster, wshot czar
WFSB Finance Group	Power User	Board Finance Staff, Mitzi Gearhart
WFSB User Group	User	Board Staff, Ashley Holt-Patterson, Mitzi Gearhart, Brian Divers, Networx Divers
WFSB VPN Access Group	User	Limited Board Staff, Networx Divers
WFSC VPN Access Group	User	
Tech Dept Account Managers Group	Administrator	IT, Ed Newman
HOTWIFI	Administrator	Meraki Admin
O365 Self-Service Portal	User	
BSU Admin Group	Power User	BSU Staff
BSU Solutions Public Group	User	
BSU Staff Group	User	BSU Staff
CCS Share Group	User	Child Care Staff
CCS Users	User	Child Care Staff
CECT Users	User	CECT Center Staff
WFSC Case Managers	Power User	Center Case Managers
WFSC Manager Users	Power User	Center Managers
WFSC Share Administrators Group	Administrator	WFC Mgmt
WFSC Social Network Group	User	WFC Mgmt, BSU Staff
CCS Fax Admins	User	CCS, IT
CCS Fax Group	User	CCS, IT

Frame Users	User	

Flaw Remediation
The Heart of Texas Workforce Solutions Technology Department will identify, report, and correct information system flaws.

The Heart of Texas Workforce Solutions Technology Department will test software and firmware updates related to flaw remediation for effectiveness and potential side effects before installation. The Heart of Texas Workforce Solutions Technology Department installs security-relevant software and firmware updates within 30 days of the release of the update and incorporate flaw remediation into the organizational configuration management process.

Malicious Code Protection
The Heart of Texas Workforce Solutions Technology Department will implement malicious code protection mechanisms at system entry and exit points to detect and eradicate malicious code.

The Heart of Texas Workforce Solutions Technology Department will automatically update malicious code protection mechanisms as new releases are available in accordance with organizational configuration management policy and procedures.

The Heart of Texas Workforce Solutions Technology Department will configure malicious code protection mechanisms to perform periodic scans of the information system weekly and real-time scans of files from external sources at the endpoint and/or network entry/exit points as the files are downloaded, opened, or executed in accordance with organizational security policy.

The Heart of Texas Workforce Solutions Technology Department will block malicious code, quarantine malicious code, and/or send alert to administrator in response to malicious code detection and will addresses the receipt of false positives during malicious code detection and eradication and the resulting potential impact on the availability of the system.

Information System Monitoring
The Heart of Texas Workforce Solutions Technology Department will monitor the systems to detect attacks, indicators of potential attacks, unauthorized local, network, and remote connections.

The Heart of Texas Workforce Solutions Technology Department will identify unauthorized use of the systems through the following techniques and methods:

- Log capture & monitoring
- SOC services

The Heart of Texas Workforce Solutions Technology Department will invoke internal monitoring capabilities or deploy monitoring devices strategically within the information system to collect organization-determined essential information and at ad hoc locations within the system to track specific types of transactions of interest to the organization.

The Heart of Texas Workforce Solutions Technology Department will analyze detected events and anomalies.

The Heart of Texas Workforce Solutions Technology Department will adjust the level of system monitoring activity whenever there is a change in risk to organizational operations and assets, individuals, other organizations, or the nation based on law enforcement information, intelligence information, or other credible sources of information.

The Heart of Texas Workforce Solutions Technology Department will obtain legal opinion regarding the system monitoring activities.

The Heart of Texas Workforce Solutions Technology Department will provide monitoring information to authorized personnel or roles on a monthly basis, or as needed.

Security Alerts, Advisories, and Directives

The Heart of Texas Workforce Solutions Technology Department will receive system security alerts, advisories, and directives from defined external organizations on an ongoing basis and will generate internal security alerts, advisories, and directives as deemed necessary.

EXTERNAL ORGANIZATIONS
Arctic Wolf
DIR
TWC
Texas ISAO

The Heart of Texas Workforce Solutions Technology Department will disseminate security alerts, advisories, and directives to defined personnel, groups, roles and defined external organizations.

GROUPS/ROLES/EXTERNAL ORGANIZATIONS
HOTWDB Information Technology Security Steering Committee
Technology Management
Users as needed

The Heart of Texas Workforce Solutions Technology Department will implement security directives in accordance with established timeframes or notify the issuing organization of the degree of noncompliance.

Security Function Verification

The Heart of Texas Workforce Solutions Technology Department will verify the correct operation of security and privacy functions on a quarterly basis and will alert defined personnel, of failed security and privacy verification tests and tactical remediation when anomalies are discovered.

PERSONNEL
Technology Management
Affected Users
Affected Management

Software, Firmware and Information Integrity

The Heart of Texas Workforce Solutions Technology Department will employ integrity verification tools to detect unauthorized changes to authorized software, firmware, and information.

The Heart of Texas Workforce Solutions Technology Department will take the following actions when unauthorized changes to the software, firmware, and information are detected:

CHANGE DESCRIPTION	ACTION
Unauthorized software installed	Remove or block software, notify management & staff member of policy & procedures
Unauthorized hardware installed	Remove or block hardware, notify management & staff member of policy & procedures
Unauthorized information sharing	notify management & staff member of policy & procedures
Unauthorized use of personal devices accessing information	Block personal device at firewall, notify management & staff member of policy & procedures.

Spam Protection

The Heart of Texas Workforce Solutions Technology Department will employ spam protection mechanisms at system entry and exit points to detect and act on unsolicited messages. Spam protection mechanisms will be updated when new releases are available in accordance with organizational configuration management policy and procedures.

Error Handling

The Heart of Texas Workforce Solutions Technology Department will generate error messages that provide information necessary for corrective actions without revealing information that could be exploited and will reveals error messages only to those with a need to know.

Information Handling and Retention

The Heart of Texas Workforce Solutions Technology Department will manage and retain information within the information system and information output from the system in accordance with applicable federal laws, Executive Orders, directives, policies, regulations, standards, and operational requirements. The default retention duration for HOTWDB documentation follows requirements set in the TWC Records and Information Management Manual.(Attachment A)

Personally Identifiable Information Quality Operations

The Heart of Texas Workforce Solutions Technology Department will check the accuracy, relevance, timeliness, and completeness of personally identifiable information across the information life cycle no less than quarterly and correct or delete inaccurate or outdated personally identifiable information.

Enforcement

Violations of this policy or failure to implement provisions of this policy may result in disciplinary action up to and including termination, civil litigation, and/or criminal prosecution.

DOCUMENT CONTROL

Document Name	Audit and Accountability
Document Control Number	TCF 12, 16, & 20
Document Identification	Version 1.0
Owner/Approver Identification	Technology Department
Author	Matilda Alonzo
Document Reviewer(s)	ITSSC
Review Plan	This document should be reviewed by all parties on a regular basis. Next review is: 3/1/2024
Distribution	The main version of this document is stored in S:\Policies\Cybersecurity> PRINTED COPIES OF THIS DOCUMENT ARE FOR REFERENCE ONLY!

REVISION HISTORY		
Date	Revised By	Changes
3/1/2023	Matilda Alonzo	Initial Release