HEART OF TEXAS WORKFORCE DEVELOPMENT BOARD, INC.

POLICY

ID NO.:	HWD CS 007-22	**DATE ISSUED:**	11/1/2022
PROGRAM:	Cybersecurity	**KEYWORD:**	Media Protection Policy

SUBJECT: Media Protection Policy

PURPOSE: To provide staff with information and guidance on media protection requirements as well as guidelines for auditing systems within the Heart of Texas Workforce Solutions environment.

REFERENCES: Texas Workforce Commission (TWC) Information Security Manual 2.0 Sept. 24, 2021 Section 3.2

POLICY: MEDIA PROTECTION

GENERAL POLICY

The Heart of Texas Workforce Development Board (HOTWDB) Technology Team will develop, document, and disseminate a media protection policy and procedures that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance.

The HOTWDB Technology Team will review and update media protection policy and procedures at least annually.

Media Access

The HOTWDB employees, contractors, and partners will restrict access to *digital and/or non-digital medi*a to *defined personnel, groups, or roles*.

GROUPS	ROLES	PERSONNEL
WFSB User Group	User	WFSB Staff
WFSB Finance Group	User	Finance Staff
Tech Dept Account Managers Group	Admin	IT Staff
O365 Self-service Password	User	CIS, CECT Mgr, IT
HOTWIFI	Admin	Meraki Admin
BSU Admin Group	Shared Mailbox User	Solutions email staff
BSU Solutions Public Group	User	BSU Staff, IT Staff
BSU Staff Group	User	BSU Staff
CCS Share Group	User	CCS Staff
CCS Users (Forcepoint monitoring)	User	CCS Staff
CECT Users	User	CECT Corporate Staff
CIS group (Forcepoint monitoring)	User	CIS Staff
WFSC Case Managers	User	Case Monitoring Staff (Rural staff)
WFSC Labuser Group	User	Lab user accounts
WFSC Manger Group	User	WFSC Managers
WFSC Resumes Group	User	WFSC Managers
WFSC Share Administrators Group	Admin	WFSC Managers, ABrobston
WFSC Share Group	User	All WFSC Staff
WFSC Social Network Group (Forcepoint)	User	Marketing Staff, BSU Staff
WFSC Staff (Forcepoint)	User	WFSC Staff
WFSC Vet Group (Forcepoint)	User	Veteran Services Staff
WFSC VPN Access Group	User	Telework Staff
Frame Admins	Admin	IT Staff

Domain Admins	Admin	IT Staff; Approved staff
Domain Users	User	All domain users
Enterprise Admins	Admin	Networx, HOTWDB czar
Enterprise Key Admins	Admin	AzureSync, PrtMgrPlus, Frame Service
Schema Admins	Admin	Networx, HOTWDB czar

Media Marking

The HOTWDB employees, contractors, and partners will mark information system media indicating the distribution limitations, handling caveats, and applicable security markings of the information system media from marking if the media remains within defined controlled areas.

MEDIA	CONTROLLED AREA	STATUS
Unexpired Backup Tapes	Safe at Region 12	Read Only
Expired Backup Tapes	IT Staff office/home	Writeable
Open case files – paper	Behind 2 locked doors	Confidentially Marked
Closed case files – paper	Behind 2 locked doors	Confidentially Marked
Digital Files with PII	Network Storage	Password Protect
Email with PII	Email System	Encrypt
Email Attachments with PII	Email System	Encrypt or Password Protect
USB Flash Drives with customer info	Locked drawer	Confidentially Marked / Data protected with pw or encryption
External Hard Drive with customer information	Locked drawer	Confidentially Marked / Data protected with pw or encryption

Media Storage

The HOTWDB employees, contractors, and partners will physically control and securely store *defined digital and/or non-digital media* within *defined controlled areas* until the media are destroyed or sanitized using approved methods.

MEDIA	CONTROLLED AREA
Unexpired Backup Tapes	Safe at Region 12
Expired Backup Tapes	WFB IT Staff office/home office
Open case files - paper	Behind 2 locked doors
Closed case files - paper	Behind 2 locked doors
USB Flash Drives with customer information	Password protected / Encrypted in Locked drawer

External Hard Drive with customer information	Password protected / Encrypted in Locked drawer
Digital Media	Network storage

Media Transport

The HOTWDB employees, contractors, and partners will protect and control *information system media* during transport outside of controlled areas using *defined security safeguards*]. The Heart of Texas Workforce Solutions employees will restrict to authorized personnel the maintenance of accountability for system media during transport outside of controlled areas and document activities associated with the transport of system media.

MEDIA	SAFEGUARD
Unexpired Backup Tapes	Data is encrypted and to remain in Safe at Region 12 until expiry.
Expired Backup Tapes	Data is encrypted and to remain in IT Staff possession only.
Open case files - paper	Sign out sheet with manager approval should be completed when files leave the building. File documents must be kept together in file folder.
Closed case files - paper	Sign out sheet with manager approval should be completed when files leave the building. File documents must be kept together in file folder.
USB Flash Drives with PII	USB drive must be encrypted or have password protection.
External Hard Drive with PII	USB drive must be encrypted or have password protection.

Media Sanitization

The HOTWDB employees, contractors, and partners will sanitize *information system media* prior to disposal, release out of organizational control, or release for reuse using *authorized sanitization techniques and procedures* in accordance with applicable federal and organizational standards and policies. The sanitization mechanisms with the strength and integrity commensurate with the security category or classification of the information.

Media Use

The HOTWDB Leadership team *prohibits* the use of *defined types of information system media* on *defined information systems or system components* using *defined security safeguards*.

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	Media Protection
Document Control Number	TCF 23
Document Identification	Version 1.0
Owner/Approver Identification	Technology Department
Author	Matilda Alonzo
Document Reviewer(s)	
Review Plan	This document should be reviewed by all parties on a regular basis. Next Review is: 11/1/2023
Latest Version	
Distribution	The master 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
11/1/2022~~3~~	Matilda Alonzo	Initial release.