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

HEART OF TEXAS WORKFORCE DEVELOPMENT BOARD, INC.

POLICY

ID NO.:	HWD CS 008-22	**DATE ISSUED:**	11/1/2022
PROGRAM:	Cybersecurity	**KEYWORD:**	Identification & Authorization Policy

SUBJECT: Identification & Authorization Policy

PURPOSE: To provide staff with information and guidance on the Identification and Authorization expectations and oversight within the Heart of Texas Workforce Solutions environment.

REFERENCES: TWC Information Security Manual Version 2.0 Section 3.2.20
POLICY: IDENTIFICATION & AUTHORIZATION POLICY

GENERAL POLICY

Heart of Texas Workforce Development Board's (HOTWDB) Technology Department will develop, document, and disseminate an Identification and Authentication policy and procedures that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance.

HOTWDB's Technology Department will review and update the current Identification and Authentication policy and procedures at least annually.

Identification and Authentication (Organizational Users)
The information system uniquely identifies and authenticates organizational users (or processes acting on behalf of organizational users).

Device Identification and Authentication
The information system uniquely identifies and authenticates *specific and/or types of devices* before establishing a local, remote, or network connection.

Identifier Management
HOTWDB's Technology Department will manage information system identifiers by receiving authorization from a *defined authority* to assign an individual, group, role, or device identifier.

HOTWDB's Technology Department will manage information system identifiers by selecting an identifier that identifies an individual, group, role, or device.

HOTWDB's Technology Department will manage information system identifiers by assigning the identifier to the intended individual, group, role, or device.

HOTWDB's Technology Department will manage information system identifiers by preventing reuse of identifiers for 30 Days and will disable the identifier after 90 Days & 180 days delete of inactivity.

Authenticator Management
HOTWDB's Technology Department will manage information system authenticators by verifying, as part of the initial authenticator distribution, the identity of the individual, group, role, or device receiving the authenticator.

HOTWDB's Technology Department will manage information system authenticators by establishing initial authenticator content for authenticators defined by the organization.

HOTWDB's Technology Department will manage information system authenticators by ensuring that authenticators have sufficient strength of mechanism for their intended use.

HOTWDB's Technology Department will manage information system authenticators by establishing and implementing administrative procedures for initial authenticator distribution, for lost/compromised or damaged authenticators, and for revoking authenticators.

HOTWDB’s Technology Department will manage information system authenticators by changing default content of authenticators prior to information system installation.

HOTWDB’s Technology Department will manage information system authenticators by changing/refreshing authenticators as listed below:

AUTHENTICATOR TYPE	FREQUENCY
Active Directory	90 Days
Windows Local Admin Accounts (Desktops)	annually
Windows Local Admin Accounts (Laptops)	annually
Windows Local User Accounts (Desktops)	90 Days
Windows Local User Accounts (Laptops)	90 Days
Network Devices	annually
Apple Devices	90 Days
Web Accounts	90 Days

HOTWDB’s Technology Department will manage information system authenticators by protecting authenticator content from unauthorized disclosure and modification.

HOTWDB’s Technology Department will manage information system authenticators by requiring individuals to take, and having devices implement, specific security safeguards to protect authenticators.

HOTWDB’s Technology Department will manage information system authenticators by changing authenticators for group/role accounts when membership to those accounts change.

Authenticator Feedback
The information system obscures feedback of authentication information during the authentication process to protect the information from possible exploitation/use by unauthorized individuals.

Cryptographic Module Authentication
The information system implements mechanisms for authentication to a cryptographic module that meet the requirements of applicable federal laws, Executive Orders, directives, policies, regulations, standards, and guidance for such authentication.

Identification and Authentication (Non-organizational Users)
The information system uniquely identifies and authenticates non-organizational users (or processes acting on behalf of non-organizational users).

DOCUMENT CONTROL

Document Name	Identification & Authorization
Document Control Number	TCF 28 & 29
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 <11/2023>
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	Matilda Alonzo	Initial Release