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

HEART OF TEXAS WORKFORCE DEVELOPMENT BOARD, INC.

**POLICY**

| | | | |
|---|---|---|---|
| **ID NO.:** | HWD CS 017-23 | **DATE ISSUED:** | 6/1/2023 |
| **PROGRAM:** | Cybersecurity | **KEYWORD:** | Access Control Policy |

**SUBJECT:** Access Control Policy

**PURPOSE:** To provide staff with information and guidance on Access Control requirements as well as guidelines for access Technology and Information Resources within the Heart of Texas Workforce Solutions environment.

**REFERENCES: Security Control Standards Catalog Texas Department of Information Resources Version 2.0 Effective Date 1/20/22; TWC Information Security Manual v3.0**

**POLICY: ACCESS CONTROL POLICY**

## GENERAL POLICY

Heart of Texas Workforce Solutions Development Board, Inc. (HOTWDB) Information Technology Security Steering Committee (ITSSC) is responsible for developing, documenting and disseminating Access Control consistent with applicable laws, executive orders, directives, regulations, policies, standards and guidelines. The Document Owner is responsible for the maintenance and periodic review of this document.

The purpose of this policy is to ensure security controls are in place, effective, and are not being bypassed. Groups and Roles will be defined in alignment with the Heart of Texas Workforce Solutions computing structure and will define criteria for group membership with defined prerequisites and criteria for assignment.

This policy applies to all HOTWDB staff and contractors; on all HOTWDB owned, leased, operated or other maintained information systems operated by or on behalf of HOTWDB; and for all stored, processed, or transmitted HOTWDB data.

The HOTWDB Technology Department will ensure:

1. The segregation of duties is enforced physically and logically where appropriate.
2. Ensure that procedures address the maintenance of appropriate segregation of duties and responsibilities during periods when regular personnel are unavailable (e.g., vacations, illness or leaves of absence).
3. Document separation of duties of personnel.
4. Review the impact on segregation of duties and reassign responsibilities where necessary when job roles and responsibilities are created or updated as a result of changing business needs or reorganization.
5. Provide personnel the ability to have access to their personally identifiable information (PII) maintained in its system(s) of records.
6. Publish rules and regulations governing how personnel may request access to records maintained in a Privacy Act system of records.
7. Define, document, approve, and enforce physical and logical access restrictions associated with changes to the information system.
8. Prohibit any activity which may harass, threaten, or abuse others, degrade the performance of information resources, deprive, or reduce an authorized User's access to resources or otherwise circumvent any security measure or policy is prohibited. Including:
9. Prohibit the intentional access, creation, storage, or transmission of any material that may be offensive, indecent, or obscene unless such action is specifically within the scope of job duties for their position.
10. Require approval by the Cybersecurity Coordinator or authorized Technology Department staff for connection of non-government furnished or contractor-owned IT devices (including Universal

Serial Bus (USB)-connected portable storage and mobile devices) to agency-owned systems or networks receiving, processing, storing, accessing, protecting and/or transmitting confidential or sensitive data. This requirement does not apply to networks and systems intended for use by the general public.

Only authorized users are permitted to have access to the systems associated with their roles and responsibilities as defined by the HOTWD IT Leadership. Access requests must be reviewed and approved by a defined and authorized independent party in compliance with separation of duties practices. The list of Authorized personnel can be found below.

| | |
|---|---|
| Approver | IT Staff Representative |
| Approver | Cybersecurity Coordinator |
| Approver | IT Contract Manager |

**User Accounts**

The creation, modification, and deletion of accounts must follow defined procedures and conditions. All accounts must have an assigned account manager. User accounts must be assigned to groups. The groups will follow the least privileged principle and will be applied uniformly.

Notification of changes in account status will be communicated to the defined approvers for:

1. Within <24 hours> from when Accounts are no longer needed
2. Immediately upon termination
3. Within <24 hours> from a shift in responsibility in line with least privileged access principles

The authorization to systems will require:

1. Access authorization from a defined approver; and,
2. Identification of the required group and associated resources

To ensure account hygiene Periodic business reviews of account compliance will occur at least annually.

Temporary and Emergency Accounts will be removed after 72 hours of issuance, or upon completion of the user need. Any exceptions to this policy must be accompanied with formal approval prior to issuance of the temporary or emergency-based credentials.

Enforcement of approved authorizations for logical access and system resources will be done in accordance with applicable access control policies in a uniform manner. The enforcement will control the flow of information within the system and between connected systems based on the group permissions and access requirements of the specific user or group. The principles of least privilege will be employed, allowing only authorized access for users that are necessary to accomplish assigned organizational tasks.

**Unsuccessful Logins**

5 of unsuccessful login attempts by a user in succession will automatically lock the account until released automatically, or by an authorized administrator when exceeded.

**System Use Notification**

Systems will display a banner prior to login with security and privacy notices consistent with applicable laws, executive orders, directives, policies, and standards stating:

1. Users are accessing government systems
2. System usage may be monitored, recorded, and audited
3. Unauthorized use of the systems is prohibited and subject to criminal and civil penalties
4. Use of the system indicates consent to monitoring and recording

**Device Lock**

Devices will automatically lock after 15 minutes of inactivity and are required to bemanual locked before leaving a device unattended.The lock will remain until the user re-establishes access using their authorized credentials.

**VPN Session Termination**

User sessions will automatically terminate after 12 hours of inactivity. Users will be required to re-establish the session after the user re-establishes access using their authorized credentials.

**Remote Access**

HOTWDB IT Leadership will establish and document usage restrictions, configuration requirements and implementation guidance for each type of allowed access. Documentation can be foundat S:\Procedures\Cybersecurity

**Wireless Access**

HOTWDB IT Leadership will establish and document usage restrictions, configuration requirements and implementation guidance for each type of allowed access. Documentation can be found at S:\Procedures\Cybersecurity.Wireless access must be authorized prior to allowing access to Heart of Texas Workforce Solutions resources.

**Access Control for Mobile Devices**

HOTWDB IT Leadership will establish and document usage restrictions, configuration requirements and implementation guidance for each type of allowed access to include when such devices are outside of controlled areas. Documentation can be found below or at S:\Procedures\Cybersecurity .
Mobile access must be authorized prior to allowing access to Heart of Texas Workforce Solutions resources.

**Use of external systems and Bring Your Own Device (BYOD)**

HOTWDB IT Leadership will establish controls that establish that the external system is consistent with the trust relationships established with other organizations or persons owning, operating, and/or maintaining external systems, allowing authorized individuals to access the system from external systems; and process, store, or transmit organization-controlled information using external systems.

**Information Sharing**

Authorized users will determine whether access authorizations assigned to a sharing partner match the information’s access and use restrictions for defined information sharing circumstances where user discretion is required and employ organization-defined automated mechanisms or manual processes to assist users in making information sharing and collaboration decisions.

**Publicly Accessible Information**

HOTWDB Leadership will designate authorized users or roles to make information publicly available. HOTWDB Leadership will train the authorized users on what consists of non-public information for effective execution of their responsibilities.  Content will be reviewed by the appointed personnel to and after posting for non-public content.  All non-public content will be removed upon identification.

## EXCEPTIONS

Any exceptions to this policy must be approved via the HOTWDB Security Exception guideline.

## 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 | Access Control |
| Document Control Number | TCF #29 |
| Document Identification | Version 1.0 |
| Owner/Approver Identification | HOTWDB ITSSC |
| Author | Matilda Alonzo |
| Document Reviewer(s) | HOTWDB ITSSC |
| Review Plan | This document should be reviewed by all parties on a regular basis.<br>Next Review is: 5/24/2024 |
| 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 |
| 6/1/2023 | Matilda Alonzo | Initial release. |
| | | |