



HEART OF TEXAS WORKFORCE DEVELOPMENT BOARD, INC.

POLICY

ID NO.:	HWD CS 006-22	DATE ISSUED:	11/1/2022
PROGRAM:	Cybersecurity	KEYWORD:	Physical & Environmental Protection Policy

SUBJECT: Physical & Environmental Protection Policy

PURPOSE: To provide staff with information and guidance for both physical security and environmental protection requirements within the Heart of Texas Workforce Solutions environment.

REFERENCES: TWC Information Security Manual Version 2.0 Section 3.2.10

POLICY: PHYSICAL AND ENVIRONMENTAL PROTECTION POLICY

GENERAL POLICY

The Heart of Texas Workforce Development Board (HOTWDB) Information Technology Security Steering Committee team will develop, document, and disseminate a Physical and Environmental Protection policy and procedures that address purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance.

The HOTWDB Information Technology Security Steering Committee will review and approve the Physical and Environmental Protection policy and procedures at least annually.

Physical Access Authorizations

HOTWDB management or designated representative will develop, approve, and maintain a list of individuals with authorized access to the facility where the information system resides.

HOTWDB site management or designated representative will issue authorization credentials for facility access.

HOTWDB site management or designated representative will review the access list detailing authorized facility access by individuals at least every 30 days and remove individuals from the facility access list when access is no longer required.

HOTWDB site management or designated representative will remove individuals from the facility access list when access is no longer required.

Physical Access Controls

HOTWDB site management or designated representative will enforce physical access authorizations at defined entry/exit points to the facility where the information system resides by verifying individual access authorizations before granting access to the facility and controlling ingress/egress to the facility using physical access control systems/devices or guards.

HOTWDB site management or designated representative will maintain physical access audit logs for defined entry/exit points.

HOTWDB site management or designated representative will control access to areas within the facility officially designated as publicly accessible.

HOTWDB site management or designated representative will escort visitors and monitor visitor activity.

HOTWDB site management or designated representative will secure keys, combinations, and other physical access devices.

HOTWDB site Technology team will inventory physical access devices at least every 12 months.

HOTWDB site management or designated representative will change combinations annually. Combinations and/or master keys will be changed when keys are lost, combinations are compromised, or individuals are transferred or terminated.

Access Control for Transmission Medium

HOTWDB site management or designated representative will control physical access to information system distribution and transmission lines within organizational facilities using security safeguards.

Access Control for Output Devices

HOTWDB site management or designated representative will control physical access to output from devices to prevent unauthorized individuals from obtaining the output.

Monitoring Physical Access

HOTWDB site management or designated representative will monitor physical access to the facility where the information system resides to detect and respond to physical security incidents.

HOTWDB site management or designated representative will review physical access logs weekly and upon occurrence of security related *events or potential indications of security related events*.

HOTWDB site management or designated representative will coordinate the results of reviews and investigations with the organizational incident response capability.

Power Equipment and Cabling

The HOTWDB Technology Department will protect power equipment and power cabling for the information system from damage and destruction.

Emergency Shutoff

The HOTWDB Technology Department will provide the capability of shutting off power to the information system or individual system components in emergency situations.

The HOTWDB Technology Department will place emergency shutoff switches or devices to facilitate safe and easy access for personnel.

The HOTWDB Solutions Technology Department will protect emergency power shutoff capability from unauthorized activation.

Emergency Power

The HOTWDB Solutions Technology Department will provide a short-term uninterruptible power supply to facilitate an orderly shutdown of the information system or a transition of the information system to long-term alternate power in the event of a primary power source loss.

Emergency Lighting

HOTWDB site management or designated representative will employ and maintain automatic emergency lighting for the information system that activates in the event of a power outage or disruption and that covers emergency exits and evacuation routes within the facility.

Fire Protection

HOTWDB management or designated representative will employ and maintain fire suppression and detection devices/systems for the information system that are supported by an independent energy source.

Environmental Controls

The HOTWDB Technology Department will maintain temperature and humidity levels within the facility where the information system resides at *acceptable levels* and monitors temperature and humidity levels at least daily.

The HOTWDB Technology Department will monitor environmental control levels no less than weekly.

Water Damage Protection

The HOTWDB Technology Department will protect the information system from damage resulting from water leakage by providing master shutoff or isolation valves that are accessible, working properly, and known to key personnel.

Delivery and Removal

The HOTWDB Technology Department will authorize, monitor, and control information system components entering and exiting the facility and maintains records of those items.

Alternate Worksite

HOTWDB management or designated representative will determine and document the alternate work sites allowed for use by employees.

HOTWDB management or designated representative will employ equivalent security controls at alternate work sites.

HOTWDB management or designated representative will assess as feasible, the effectiveness of security controls at alternate work sites.

HOTWDB will provide a means for employees to communicate with information security personnel in case of security incidents or problems.

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	Physical and Environmental Protection
Document Control Number	TCF #24
Document Identification	Version 1.0
Owner/Approver Identification	IT Department
Author	Matilda Alonzo
Document Reviewer(s)	
Review Plan	This document should be reviewed by all parties on a regular basis. Next Review is: 11/1/2022
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.