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

HEART OF TEXAS WORKFORCE DEVELOPMENT BOARD, INC.

POLICY

ID NO.:	HWD CS 003-22	**DATE ISSUED:**	9/1/2022
PROGRAM:	Cybersecurity	**KEYWORD:** Cloud Usage Policy	

SUBJECT: Cloud Usage Policy

PURPOSE: To provide staff with information and guidance on Cloud Usage requirements within the Heart of Texas Workforce environment.

REFERENCES: TWC Information Security Manual 3.1.8(Department of Commerce Cloud Computing Policy)

POLICY: CLOUD USAGE POLICY

INTRODUCTION

Use of cloud computing services may introduce security challenges and the Organization must manage how the cloud provider secures and maintains the computing environment and information assets. These guidelines identify the procedures and responsibilities in the engagement and management of cloud computing services.

Cloud computing can provide highly available, convenient and on-demand access to a shared pool of computing resources (e.g. networks, servers, storage, applications and services) via the Internet. Services typically take the form of three service models (SaaS, PaaS, IaaS) that may be deployed as a public cloud available to the general public; a private cloud operated exclusively for a single organization; a community cloud available to multiple organizations with common privacy, security or regulatory requirements; or a hybrid cloud combining two or more clouds where each member is a unique entity but bound to others that enable application and data portability between them:

Software as a Service (SaaS) – Consumer uses the provider's applications running on a cloud infrastructure through client devices via web browser or program interface. The consumer does not control the underlying cloud infrastructure including network, servers, operating systems, and storage.

Platform as a Service, (PaaS) – Capability for the consumer to deploy and control applications onto the cloud infrastructure, but the consumer does not manage or control the underlying cloud network, servers, operating systems, and storage.

Infrastructure as a Service (IaaS) - Capability for the consumer to provision processing, storage, networks, and other fundamental computing resources where the consumer can deploy and run software including operating systems and applications. The consumer does not manage the underlying cloud infrastructure but has control over operating systems, storage, deployed applications, and possibly limited control of some network components such as host firewalls.

GENERAL POLICY

The organization's purchasing representative is responsible for reviewing and negotiating contract terms. The Procurement Representative will identify and work with the relevant Contract Manager to broadly define service goals and define data not limited to but including sensitivities; service level requirements and/or the sharing of such responsibilities; negotiate language, price and delivery contract terms; and get final departmental and tax approval.

Depending on data sensitivities and processing requirements, the Purchasing Representative will review and negotiate contract terms to ensure that applicable contract terms are included to meet regulatory requirements. federal and state. (e.g., Family Educational Rights and Privacy Act of 1974 (FERPA), Health Insurance Portability and Accountability Act (HIPAA), Gramm-Leach-Bliley Act (GLBA), Release of Social Security Number, Notice of Security Breach); industry-specific contractual requirements such as Payment Card Industry Data Security Standard (PCI-DSS), European Union General Data Protection Regulation (GDPR), or other requirements that may impact the Organization.

The purchasing department will work with the IT department as early as possible in the contract negotiation process. The IT department will perform a vendor security review to ensure that the vendor meets the minimum-security requirements for the organization's data. The IT department processes the bid procurement checklist and specifications before signing the contract.

IT Security & Policy

Information Assurance - Prior to contract signature, the Technology Department will perform a vendor security review aligned with common security frameworks such as National Institute of Standards and Technology (NIST) and Cloud Security Alliance (CSA) Controls Matrix, as well as, Organizational policies, standards and data handling guidelines. As part of the review, the vendor is requested to provide any applicable and available third-party security attestations or certifications (e.g. SOC-2, PCI AOC, etc.).

Based on the classified sensitivity of the data, the review will result in a report identifying controls and risks, effectiveness of those controls or recommendations for controls to mitigate risk. The Technology Department will provide the report to the Contract Relationship Owner for their review of recommendations to either proceed or consider risk mitigating controls.

If necessary, the Technology Department will provide guidance to the Contract Relationship Owner in their review of Service and Organization Controls (SOC) Reports or other third-party attestations, if applicable.

Identity and Access Management – The Technology Department will provide authentication and authorization integration services into technology infrastructure.

Contractual owner
To effectively manage the services provided by cloud computing providers, the contractual owner ("contractual owner") is identified at the time of purchase. The contractual owner has the following responsibilities:

- Performing ongoing management of the vendor engagement, deliverables, and relationship including monitoring vendor and performance to service level agreements and adherence to terms of data protection, including but not limited to:
    - availability time and service outages
    - routine maintenance timeframes
    - hardware & software updates
    - application management
    - change control
    - network controls & management
    - data confidentiality
    - data integrity
    - data availability
    - data transmission and storage encryption
    - user access controls
    - physical and/or data center security controls
    - privacy consents and notifications
    - audit requirements, including annual review of SOC 2 or other required 3rd party attestations
    - assurance of supply chain or other third-party services providers supporting the cloud service provider
    - disaster recovery and business continuity
- Initiating dialog to address any performance issues directly with the vendor and collaborate with other Organizational units as needed, including
- Supporting timely and accurate payment, and engage the Purchasing Department in contract renewals, amendments, or termination.

DOCUMENT CONTROL

Document Name	Cloud Usage
Document Control Number	TCF Control #8
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: <9/1/2022>
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
9/1/2022	Matilda Alonzo	Initial release.