

Request for Offers

Managed Services – College and Career Advising No. 781-6-CB-20

Technical Categories

1.	Application Development, Maintenance, and Support
2.	Comprehensive Web Development and Management Services
3.	Managed Services

NIGP Code(s):

915-96	Webpage Design, Management & Maintenance
920-00	Data Processing, Computer, and Software Services
920-40	Programming Services, Computer, Including Mobile Device Applications
920-65	System Requirements, Quality Assurance Review
208-54	Internet, Web Site and Mobile Application Development Software, Microcomputer
958-77	Project Management

Important Dates:

RFO Post Date:	October 1, 2026
Written Questions Due:	October 9, 2026, by 11:30 PM CT
Proposal Deadline:	October 22, 2026, by 11:30 PM CT

Texas Higher Education Coordinating Board
1801 N. Congress Ave., Suite 12.200
Austin, Texas 78701

Table of Contents

1.	Introduction.....	1
1.1	Overview	1
1.2	Definitions	2
1.3	Authority and Attachments.....	2
2.	Contract Term and Authorization.....	3
2.1	Contract Term	3
2.2	Contract Work Authorization	3
3.	Minimum Eligibility and Experience Requirements.....	4
4.	Statement of Work.....	4
4.1	Overview	4
4.2	Technology Environment.....	5
4.2.1	Technology Portfolio	5
4.2.2	Current Technology Stack.....	7
4.2.3	External Integrations	8
4.2.4	Application Usage.....	8
4.2.5	Supporting Enterprise Technologies.....	8
4.2.6	Technology Evolution.....	9
4.2.7	Technology Environment Disclaimer	10
4.3	Delivery Organization Model and Team Structure.....	10
4.4	Delivery Organization Staffing Requirements.....	11
4.4.1	Personnel Management	12
4.4.2	Key Personnel and Staffing Continuity.....	13
4.4.3	Personnel Performance and Security	14
4.4.4	Remote, Nearshore, and Offshore Resources.....	14
4.5	Managed Services	15
4.5.1	Application Operations and Maintenance	16
4.5.2	Application Development and Enhancement.....	17
4.5.3	Solution Architecture and Technical Design	19
4.5.4	Quality Engineering.....	22
4.5.5	DevScOps and Release Management.....	24
4.5.6	Cloud Operations and Infrastructure.....	27

4.5.7	Security and Compliance.....	29
4.5.8	Documentation and Knowledge Management.....	31
4.5.9	Agile Delivery Management.....	33
4.5.10	Continuous Improvement and Innovation	35
4.6	Governance.....	36
4.6.1	Governance Model	37
4.6.2	Governance Meetings and Communication.....	39
4.6.3	Communication and Escalation	41
4.7	Performance Management and Service Reporting.....	41
4.7.1	Performance Management.....	41
4.7.2	Performance Reporting.....	42
4.8	Service Readiness, Transition, and Continuity.....	43
4.8.1	Service Transition and Operational Readiness	44
4.8.2	Ongoing Service Transition	45
4.8.3	Service Transition and Contract Closeout.....	46
4.9	Deliverables.....	47
5.	Security Requirements.....	48
5.1	Security Certifications and Compliance.....	48
5.2	Security Documentation.....	49
5.3	Administrative Security Requirements.....	49
6.	Contract Administration.....	50
6.1	Deliverable Review and Acceptance	50
6.2	Contract Change Management	51
6.3	Contract Administration.....	52
6.4	Vendor Accountability	53
7.	Pricing and Payment Term.....	53
7.1	Pricing Structure.....	53
7.2	Pricing Schedule.....	55
7.3	Invoicing and Payment	55
8.	Solicitation Key Deadlines and Events.....	57
8.1	Procurement Schedule.....	57
8.2	Proposal Due Date	57

8.3	Procurement Point of Contact	58
8.4	Questions and Answers	58
8.5	Proposal Submission	59
8.6	Proposal Modification and Withdrawal	59
9.	Proposal Submission Requirements	60
9.1	Executive Summary	61
9.2	Company References.....	61
9.3	Company Experience.....	62
9.4	Delivery Organization and Key Personnel	63
9.4.1	Delivery Organization.....	63
9.4.2	Key Personnel.....	64
9.5	Technical Proposal	65
9.5.1	Delivery Organization.....	65
9.5.2	Service Delivery Approach.....	66
9.5.3	Agile Delivery Methodology	66
9.5.4	Technical and Engineering Approach.....	66
9.5.5	Governance and Performance Management.....	66
9.5.6	Service Transition.....	66
9.5.7	Innovation and Continuous Improvement	66
9.6	Pricing Proposal	67
9.7	Exceptions, Assumptions, and Risks.....	67
9.8	Required Forms, Certifications, and Disclosures	68
9.8.1	Attachment A - Respondent Info	68
9.8.2	Conflict of Interest Disclosure Statement	68
10.	Proposal Evaluation	69
10.1	Evaluation Criteria	69
10.1.1	Technical Proposal and Managed Services Approach.....	69
10.1.2	Organizational Qualifications, Experience, and Past Performance	70
10.1.3	Delivery Organization and Key Personnel.....	70
10.1.4	Pricing Proposal.....	70
10.1.5	Responsiveness, Clarity, and Organization of the Proposal	71
10.2	Proposal Scoring Methodology.....	71

10.3	Scoring and Evaluation Process.....	72
10.3.1	Administrative Review.....	72
10.3.2	Evaluation.....	72
10.3.3	Clarifications, Oral Presentations, and Interviews	72
10.3.4	Contract Award	73
10.4	Best Value Determination.....	74
11.	Terms and Conditions.....	75
11.1	Costs Incurred	75
11.2	Waiver of Errors.....	76
11.3	Acceptance of Evaluation Process	76
11.4	Protest Procedures.....	76
11.5	Public Information Act	76
11.6	Retention of Proposals	77
11.7	Intellectual Property and Indemnification	77
11.8	Responsible Use of Artificial Intelligence.....	78
11.8.1	General Prohibition	78
11.8.2	Request for Approval.....	78
11.8.3	Compliance Requirements.....	79
11.8.4	Unauthorized Use and Remedies.....	79
11.8.5	AI Assisted Capabilities and Tools	80
11.9	Electronic and Information Resources Accessibility.....	80
	Appendix A – Glossary of Terms and Acronyms.....	83
	Appendix B – Information Security Standards.....	88
	Appendix C	94

1. Introduction

1.1 Overview

The Texas Higher Education Coordinating Board (THECB) is the state agency responsible for providing leadership, coordination, and strategic direction for higher education in Texas. Through its statewide strategic plan, *Building a Talent Strong Texas*, THECB is working to strengthen the state's workforce, economy, and future by increasing educational attainment for learners of all ages, expanding access to credentials of value, and advancing research and innovation.

To advance these strategic objectives, THECB develops, operates, and continuously enhances a portfolio of digital products and technology platforms that supports students, families, educators, counselors, advisors, institutions of higher education, employers, and workforce partners throughout Texas. These products improve access to higher education, simplify the admissions process, strengthen college and career advising, and connect educational pathways with workforce opportunities. The current technology portfolio includes, but is not limited to, ApplyTexas, My Texas Future, ADVi, Direct Admissions, Salesforce-based applications, Azure-hosted applications, enterprise integrations, application programming interfaces, databases, reporting platforms, and supporting cloud services.

Modern, secure, and scalable technology is essential to achieving THECB's mission. Through this Request for Offers (RFO), THECB is seeking one or more long-term technology partners to provide Managed Services supporting the ongoing operation, maintenance, enhancement, and modernization of this technology portfolio.

The selected vendor(s) shall serve as a strategic technology partner(s) by applying mature software engineering practices, disciplined delivery governance, operational excellence, and continuous improvement to ensure the technology portfolio remains secure, reliable, accessible, scalable, maintainable, and responsive to the evolving needs of the State of Texas. THECB seeks partners that will not only execute requested work but also provide technical leadership, engineering expertise, and recommendations that strengthen the long-term quality, sustainability, and operational maturity of the technology portfolio.

THECB reserves the right to award multiple contracts under this RFO and may assign products, workstreams, technologies, or specialized services among multiple vendors as determined to be in the best interest of the State of Texas.

1.2 Definitions

For the purposes of this RFO and any resulting Contract, the following terms shall apply throughout this RFO.

- **CUSTOMER** means the Texas Higher Education Coordinating Board , the State of Texas agency issuing this RFO and the recipient of all services provided under any resulting Contract.
- **RESPONDENT(S)** means an individual, partnership, corporation, limited liability company, joint venture, or other legal entity submitting a response to this RFO.
- **VENDOR** means the **RESPONDENT** selected by **CUSTOMER** and awarded a Contract pursuant to this RFO. **VENDOR** is responsible for providing all services, personnel, deliverables, reporting, governance, and other contractual obligations described in this RFO and any resulting Contract.

References to **CUSTOMER** and **VENDOR** throughout this RFO identify the respective roles, responsibilities, rights, and contractual obligations of each party. These defined terms are intended to clearly distinguish procurement requirements applicable to **RESPONDENTS** during the RFO process from contractual obligations that become applicable to the successful **VENDOR** upon Contract award.

1.3 Authority and Attachments

CUSTOMER is authorized to issue this RFO and enter into any resulting Contract pursuant to Tex. Educ. Code § 61.067 and other applicable provisions of Texas law. **RESPONDENTS** shall comply with all applicable federal and state laws and procurement requirements in preparing and submitting a response to this RFO.

This RFO is comprised of the following:

- **RFO No. 781-6-CB-20**
- **Appendix A** – Glossary of Terms and Acronyms
- **Appendix B** – Information Security Requirements
- **Appendix C** – Vendor Program (VetHUB) Participation Requirements
- **Attachment A** – Conflict of Interest Disclosure Statement (to be completed by **RESPONDENT**)
- **Attachment B** – Execution of Proposal (to be completed by **RESPONDENT**)
- **Attachment C** – Sample THECB Contract

- **Attachment D** – Certificate of Interested Parties Form 1295
- **Attachment E** – VetHUB Subcontracting Plan

RESPONDENTS are responsible for reviewing and complying with all requirements contained in these documents when preparing their responses.

2. Contract Term and Authorization

2.1 Contract Term

The anticipated Contract resulting from this RFO shall commence **upon execution** and shall terminate **August 31, 2027**, unless terminated earlier as otherwise provided for in the Contract. Following the initial Contract term, **CUSTOMER**, at its sole discretion, may renew the Contract for **up to four (4) additional one-year renewal terms** or until completion of the services authorized under the Contract, whichever occurs first. All renewals shall be made in writing and shall be subject to the terms and conditions of the Contract.

Notwithstanding the foregoing, **CUSTOMER**, at its sole discretion and upon written notice to **VENDOR**, may extend the Contract for up to twelve (12) additional months to support continuity of services, Service Transition activities, Contract closeout, procurement of replacement services, or other circumstances determined to be in the best interest of the State of Texas. Any such extension shall be performed under the terms, conditions, and pricing in effect immediately prior to the extension unless otherwise agreed to in writing by the Parties.

2.2 Contract Work Authorization

Work authorized under the Contract may include operational support, maintenance, enhancements, modernization initiatives, project-based services, emergency response activities, legislative initiatives, technical consulting, or other services described herein. **CUSTOMER** may authorize, prioritize, reprioritize, defer, accelerate, expand, reduce, suspend, or discontinue authorized work based upon changing business priorities, operational needs, legislative direction, available funding, emergency conditions, or other **CUSTOMER** requirements.

VENDOR shall support adjustments to work priorities, team capacity, and delivery schedules in accordance with the governance processes established by the Parties and shall collaborate with **CUSTOMER** to minimize operational disruption while maintaining continuity of services.

Nothing contained in the Contract shall be construed as a guarantee of any minimum quantity, dollar value, or volume of work. **CUSTOMER** reserves the

right to authorize services as needed throughout the Contract term in accordance with available funding and business priorities.

Unless otherwise specified in the Contract, work authorized under the Contract shall be planned, governed, prioritized, and delivered in accordance with the governance framework, delivery methodologies, and engineering practices established in the RFO.

3. Minimum Eligibility and Experience Requirements

This section establishes the minimum qualifications and organizational experience that each **RESPONDENT** must satisfy to be considered for award.

RESPONDENTS must demonstrate a minimum of five (5) years of experience providing Managed Services or substantially similar services comparable in scope, complexity, and technical environment to those described in this RFO. An entity or company in existence for fewer than five (5) years may submit a proposal provided its executive leadership and Delivery Organization collectively demonstrate the required experience.

RESPONDENTS that do not satisfy this minimum requirement are not eligible for award.

RESPONDENTS shall demonstrate organizational experience delivering enterprise application development, application maintenance, production support, Agile software delivery, DevSecOps, cloud operations, quality engineering, and related technology services for organizations of similar size and complexity. Experience supporting public sector organizations, cloud-based application platforms, enterprise integrations, customer-facing digital services, and modern software engineering practices is preferred.

RESPONDENTS shall demonstrate experience operating under an outcome-based Managed Services delivery model in which **VENDOR** is responsible for staffing, engineering execution, operational management, quality, service delivery, and continuous improvement while **CUSTOMER** provides governance, business priorities, product ownership, enterprise architecture oversight, and contract administration.

4. Statement of Work

4.1 Overview

VENDOR shall provide comprehensive Managed Services supporting the ongoing operation, maintenance, enhancement, and modernization of THECB's College and Career Advising technology portfolio.

This engagement will establish a long-term managed services partnership that enables **CUSTOMER** to continuously deliver secure, reliable, accessible, scalable, and user-centered digital services supporting students, families, educators, counselors, advisors, institutions of higher education, employers, and workforce partners throughout Texas.

VENDOR shall provide the necessary personnel, technical expertise, engineering practices, governance, tools, processes, and operational support to successfully deliver the services described in this Statement of Work.

VENDOR shall perform services using Agile delivery methodologies supported by modern software engineering practices, DevSecOps, automation, continuous testing, quality engineering, and continuous improvement.

VENDOR shall be responsible for the day-to-day engineering execution necessary to operate and evolve the technology portfolio, including application development, application maintenance, production support, quality engineering, release management, technical documentation, cloud operations, application security, performance optimization, and operational monitoring. **CUSTOMER** will provide product vision, business priorities, architectural governance, and contract oversight.

CUSTOMER expects **VENDOR** to operate as a strategic technology partner by applying mature engineering practices, disciplined project governance, proactive risk management, and continuous improvement throughout the Contract term. In addition to delivering requested enhancements, **VENDOR** shall proactively identify opportunities to improve application architecture, software quality, accessibility, cybersecurity, cloud operations, automation, operational efficiency, maintainability, and the overall maturity of the technology portfolio.

Recommendations for improving the technology portfolio shall be presented through the governance framework established under this RFO.

4.2 Technology Environment

4.2.1 Technology Portfolio

THECB's College and Career Advising technology portfolio consists of a suite of integrated digital products, supporting platforms, and shared technology services that help Texans explore educational opportunities, prepare for higher education, apply to participating institutions, and successfully navigate their post-secondary journey. These products represent THECB's primary business applications at the time this RFO is issued.

Although each product serves a distinct business purpose, **CUSTOMER** expects the technology portfolio to operate as an integrated ecosystem. **VENDOR** shall consider interoperability, user experience, data consistency, security, maintainability, scalability, and the long-term evolution of the portfolio when performing services under this RFO. **VENDOR** shall evaluate proposed enhancements and technical decisions in the context of their impact on the overall technology portfolio rather than on individual applications alone.

THECB's College and Career Advising technology portfolio includes:

- **My Texas Future (MTF)**

My Texas Future is **CUSTOMER**'s primary digital engagement platform for Texans planning and preparing for higher education. The platform provides students with college and career exploration resources, planning tools, personalized guidance, and access to post-secondary opportunities. MTF serves as the central point of engagement for multiple advising services and the primary digital destination supporting students throughout their college planning journey.

MTF integrates with several enterprise services, including ApplyTexas, ADVi, Direct Admissions, Salesforce, and other supporting technologies to provide a seamless user experience, improve service delivery, and reduce duplicate data entry.

- **ApplyTexas**

ApplyTexas is **CUSTOMER**'s statewide application platform that enables prospective students to apply for admission to participating Texas institutions of higher education through a centralized online application. The platform also provides functionality supporting secondary school counselors and participating institutions and is administered by **CUSTOMER** in collaboration with representatives from the Texas higher education community.

- **ADVi**

ADVi is **CUSTOMER**'s AI-powered virtual advising solution, operated through the Mainstay platform, that provides students with personalized guidance regarding college planning, admissions, financial aid, enrollment, and other higher education topics. ADVi currently integrates with ApplyTexas and is expected to continue evolving through expanded integration with other

components of the College and Career Advising technology portfolio.

- **Direct Admissions**

Direct Admissions is a feature within My Texas Future that assists eligible students in identifying participating Texas colleges and universities where they may qualify for direct admission before applying. The service simplifies the college-application process, expanding access to higher education and increasing student awareness of educational opportunities available throughout Texas.

4.2.2 Current Technology Stack

CUSTOMER's College and Career Advising technology portfolio is currently hosted across a modern cloud-based application environment consisting of multiple technologies, platforms, databases, integrations, and third-party services. **RESPONDENTS** should review the information below to better understand the current operating environment.

Technology Area	My Texas Future	ApplyTexas	Direct Admissions
Front-End Framework	React	React	React
Back-End Technologies	.NET, WordPress	Node.js, Python, WordPress	.NET, WordPress
Identity and Access Management	Azure AD B2C	Azure AD B2C	Azure AD B2C
Data Storage	Azure Cosmos DB, Azure SQL Database (Enterprise Data Warehouse), Azure Blob Storage	Azure Cosmos DB, Azure SQL Database (Enterprise Data Warehouse), PostgreSQL	Azure Cosmos DB, Azure SQL Database (Enterprise Data Warehouse), Azure Blob Storage
User Experience and Design	Figma	Figma	Figma

4.2.3 External Integrations

The current portfolio integrates with a variety of enterprise and third-party platforms, including, but not limited to:

Application	Current Integrations
My Texas Future	ADVi, Salesforce, Google Analytics, Google Maps
ApplyTexas	National Student Clearinghouse (NSC), Salesforce, Google Maps, Google Analytics, Address Validation Services
Direct Admissions	ADVi, Salesforce, Google Analytics, Google Maps

4.2.4 Application Usage

Because several products within the portfolio continue to evolve, user traffic and transaction volumes are subject to change. **RESPONDENTS** should review the following planning estimates to better understand the current operating environment.

Metric	My Texas Future	ApplyTexas
Annual Distinct Users	1,700,000	3,600,000
Peak Monthly Active Users	287,000	614,000

CUSTOMER anticipates continued growth in platform utilization throughout the Contract term. **VENDOR** shall ensure that proposed solutions, architecture, operational practices, and staffing models can support increasing demand while maintaining the service levels and performance requirements established under this Contract.

4.2.5 Supporting Enterprise Technologies

In addition to the above, the College and Career Advising technology portfolio leverages enterprise platforms, cloud services, development tools, and supporting technologies that enable application development, integration, deployment, operations, security, analytics, and user experience. These platforms include, but are not limited to:

- Microsoft Azure
- CrowdStrike

- Azure DevOps
- Microsoft Entra ID / Azure AD B2C
- Salesforce
- Snowflake
- Mainstay (ADVi)
- Figma
- Enterprise Service Bus (ESB)
- Azure Data Factory
- Git-based source code repositories
- Playwright
- Continuous Integration / Continuous Deployment (CI/CD) pipelines

VENDOR is expected to possess or acquire the technical expertise necessary to effectively support these technologies and any additional enterprise platforms adopted by **CUSTOMER** during the Contract term.

4.2.6 Technology Evolution

The environment detailed above represents **CUSTOMER**'s current technology environment at the time this RFO is issued. During the Contract term, **CUSTOMER** expects the environment to evolve in response to changing business priorities, legislative direction, security requirements, technology standards, operational needs, and continuous improvement initiatives. **CUSTOMER** may add, modernize, replace, upgrade, consolidate, or otherwise modify components of the technology stack to support these needs. **VENDOR** shall provide Managed Services supporting the evolving technology portfolio in accordance with the requirements of this RFO.

VENDOR shall also proactively recommend modernization opportunities that improve application performance, reduce technical debt, increase platform reliability, security, maintainability, scalability, operational efficiency, and long-term sustainability of the technology portfolio.

VENDOR is not expected to preserve existing technologies solely because they represent the current environment. Subject to the governance processes established under this RFO, **VENDOR** shall recommend architectural, operational, and technology improvements that advance **CUSTOMER**'s strategic objectives while minimizing unnecessary technical debt and operational risk.

4.2.7 Technology Environment Disclaimer

The technologies, platforms, frameworks, tools, and integrations identified in this section are provided for informational purposes to assist **RESPONDENTS** in preparing their proposals. These technologies represent **CUSTOMER**'s current operating environment and should not be interpreted as limiting **CUSTOMER**'s ability to adopt, retire, replace, upgrade, consolidate, or otherwise modify technologies during the term of the resulting Contract.

4.3 Delivery Organization Model and Team Structure

CUSTOMER intends to establish a long-term Managed Services partnership in which **VENDOR** is responsible for organizing, staffing, managing, and continuously improving the Delivery Organization necessary to successfully perform the services described in this RFO. **CUSTOMER** will establish business priorities, product vision, enterprise governance, and strategic direction, while **VENDOR** shall remain responsible for engineering execution, service delivery, operational management, technical leadership, and delivery outcomes.

VENDOR shall organize a Delivery Organization using cross-functional, collaborative teams possessing the technical expertise, engineering disciplines, operational capabilities, and leadership necessary to support **CUSTOMER**'s evolving technology portfolio. The Delivery Organization shall be capable of supporting the ongoing operation, maintenance, enhancement, modernization, security, quality engineering, cloud operations, and continuous improvement of the applications and technologies described in this RFO.

CUSTOMER expects **VENDOR** to utilize Agile delivery methodologies, including Scrum, Kanban, or other **CUSTOMER**-approved Agile practices, to plan, prioritize, develop, test, deploy, and support work performed under this Contract. **VENDOR** shall remain responsible for coordinating activities across multiple delivery teams, technologies, and functional disciplines to ensure integrated planning, architectural alignment, engineering consistency, release coordination, quality engineering, and operational continuity throughout the technology portfolio.

Although **CUSTOMER** will identify the capabilities and functional disciplines necessary to support this engagement, **CUSTOMER** does not prescribe the **VENDOR**'s internal organizational structure. **VENDOR** may propose any organizational model that effectively satisfies the requirements of this RFO, provided the proposed Delivery Organization demonstrates the leadership, technical expertise, staffing capacity, governance, and operational maturity necessary to successfully deliver the required services.

The Delivery Organization shall be capable of scaling resources, adjusting priorities, and supporting multiple concurrent operational, maintenance, enhancement, and modernization initiatives while maintaining service continuity, operational stability, engineering quality, and the performance standards established under this Contract.

VENDOR shall work collaboratively with **CUSTOMER**'s Product Owners, business stakeholders, enterprise architects, cybersecurity personnel, cloud administrators, and other **CUSTOMER** representatives throughout the Contract term. **VENDOR** shall actively participate in governance activities, planning sessions, architecture reviews, backlog refinement, sprint planning, release planning, demonstrations, retrospectives, and other collaborative activities necessary to support successful delivery of the services described in this RFO.

4.4 Delivery Organization Staffing Requirements

RESPONDENTS' Delivery Organization shall collectively provide the capabilities necessary to support **CUSTOMER**'s College and Career Advising technology portfolio through a combination of leadership, engineering, quality engineering, architecture, DevSecOps, cloud operations, production support, and other specialized technical disciplines required to successfully perform the services described in this Contract.

At a minimum, the Delivery Organization shall maintain capabilities supporting the following functional areas:

- Engagement Management
- Delivery / Project Management
- Product Management
- Scrum Leadership
- Solution and Technical Architecture
- Software Engineering (Front-End and Back-End)
- User Experience (UX) and User Interface (UI) Design
- Content Development and Management

- Quality Engineering, Test Automation, and Regression Testing
- DevSecOps and Cloud Engineering
- Azure Platform Administration
- Salesforce Administration and Development
- Database Administration
- Integration and Application Programming Interface (API) Development
- Data Engineering and Analytics
- Application Security
- Production Operations and Application Support
- Technical Documentation and Knowledge Management

Personnel assigned to the engagement shall possess education, professional experience, technical knowledge, and certifications appropriate to their assigned responsibilities and shall demonstrate experience supporting enterprise application development, cloud technologies, Agile software delivery, and Managed Services engagements of similar scope and complexity.

VENDOR may assign individual personnel to perform multiple functions where appropriate, provided sufficient capacity, qualifications, and expertise exist to successfully perform all required services and meet the performance standards established under this Contract.

VENDOR shall be responsible for ensuring that the collective knowledge, experience, and capacity of its assigned personnel are sufficient to successfully perform all services described in this Contract. **CUSTOMER** is procuring the capabilities of a Managed Services organization rather than the services of individual personnel.

4.4.1 Personnel Management

VENDOR shall be solely responsible for recruiting, onboarding, training, supervising, managing, evaluating, compensating, and replacing all personnel assigned to this engagement. **CUSTOMER** will establish business priorities, define product requirements, approve deliverables, and provide contract oversight but shall not supervise, direct, or manage individual **VENDOR** personnel.

VENDOR shall maintain sufficient staffing capacity to support planned enhancements, production operations, maintenance activities, incident response, release activities, legislative mandates, emergency production issues, and other authorized work under the

Contract. Upon request by **CUSTOMER**, **VENDOR** shall evaluate workload demands and propose adjustments to staffing levels, skill mix, or team composition necessary to accommodate changing business priorities, available funding, operational requirements, or technology initiatives.

VENDOR shall ensure personnel assigned to the engagement maintain current technical knowledge and receive ongoing professional development appropriate to the technologies, engineering practices, security requirements, and services supporting **CUSTOMER**'s environment.

4.4.2 Key Personnel and Staffing Continuity

VENDOR shall designate Key Personnel responsible for overall contract management, day-to-day service delivery, technical leadership, solution architecture, engineering governance, and quality engineering for the engagement. The specific job titles assigned to these responsibilities are at the discretion of **VENDOR**, provided the required responsibilities are clearly identified and assigned.

The Delivery Organization shall not become dependent upon any individual resource. **VENDOR** shall maintain staffing continuity throughout the Contract term by implementing appropriate knowledge transfer, succession planning, cross-training, documentation, and resource management practices. **VENDOR** shall make reasonable efforts to minimize unnecessary personnel turnover and ensure continuity of services.

VENDOR shall provide advance written notification to **CUSTOMER** of any proposed replacement of Key Personnel assigned to the engagement. Replacement personnel shall possess qualifications and experience substantially equivalent to or greater than those of the individual being replaced and shall be subject to **CUSTOMER** review and approval. **VENDOR** shall provide an appropriate transition period and complete all necessary knowledge transfer activities to minimize disruption to ongoing services. Except in emergency circumstances, Key Personnel shall not be replaced without prior written approval by **CUSTOMER**.

VENDOR shall ensure that Key Personnel identified for this engagement remain primarily dedicated to **CUSTOMER**'s Managed Services throughout the Contract term. Key Personnel shall not be assigned concurrently to other customer engagements in a manner

that materially impacts their availability, responsiveness, or ability to perform the responsibilities assigned under this Contract. If any Key Personnel are proposed to support multiple engagements, **VENDOR** shall disclose the allocation of effort in writing and obtain prior written approval from **CUSTOMER**. **CUSTOMER** reserves the right to require dedicated resources for critical roles when necessary to ensure continuity of services and successful delivery.

4.4.3 Personnel Performance and Security

VENDOR shall ensure that criminal background checks are completed and maintained for all personnel assigned to the engagement. **CUSTOMER** may review and screen, upon request, all criminal background check information prior to performance of services. **VENDOR** shall ensure that all personnel assigned to the project satisfy the requirements of any other security screening, confidentiality, training, and system access requirements established by **CUSTOMER** prior to being granted access to **CUSTOMER** systems, applications, or information.

If **CUSTOMER** reasonably determines that assigned personnel consistently fail to meet performance expectations, demonstrate inadequate technical competency, fail to comply with Contract requirements, or otherwise negatively impact service delivery, **CUSTOMER** may request replacement of those personnel. **VENDOR** shall propose qualified replacement personnel within a mutually agreed-upon timeframe and shall ensure continuity of services during the transition.

4.4.4 Remote, Nearshore, and Offshore Resources

CUSTOMER supports a hybrid workforce and recognizes that the **VENDOR** may utilize a combination of on-site and remote resources to successfully perform the services described in this Contract. **RESPONDENT** shall clearly identify its proposed staffing model, including the primary work location of personnel assigned to the engagement, as part of its Proposal.

All personnel performing services under this Contract, including subcontractors, shall be physically located within the United States and legally authorized to work in the United States. The use of nearshore, offshore, or other personnel located outside the United States is prohibited unless expressly authorized in writing by **CUSTOMER**. Upon request, **VENDOR** shall provide documentation demonstrating compliance with this requirement

Regardless of where services are performed within the United States, **VENDOR** shall remain fully responsible for the quality, security, responsiveness, communication, collaboration, and timely delivery of all services provided under this Contract. The use of remote resources shall not relieve **VENDOR** of any contractual responsibilities or performance obligations.

4.5 Managed Services

VENDOR shall provide comprehensive Managed Services supporting **CUSTOMER's** College and Career Advising technology portfolio. Services shall include the ongoing operation, maintenance, enhancement, modernization, administration, support, and continuous improvement of the applications, platforms, integrations, databases, cloud infrastructure, and supporting technologies identified in this RFO.

VENDOR shall perform all services using mature software engineering practices, Agile delivery methodologies, DevSecOps principles, and industry best practices to deliver secure, reliable, accessible, scalable, maintainable, resilient, and high-quality technology solutions.

The service areas described in this section are complementary and collectively define **VENDOR's** responsibilities for delivering Managed Services under this Contract. The responsibilities identified within each subsection establish **CUSTOMER's** minimum expectations and shall not be interpreted as limiting **VENDOR's** responsibility to perform any activity reasonably necessary to successfully operate, support, maintain, secure, enhance, modernize, or continuously improve **CUSTOMER's** technology portfolio in accordance with this RFO.

Throughout the Contract term, **VENDOR** shall proactively identify and recommend opportunities for modernization and improvement across the technology environment, including but not limited to:

- Improving the application and cloud architecture and increasing maturity of cloud environment;
- Standardizing and improving engineering practices;
- Improving release quality, deployment frequency, operational resilience, recovery time, release governance, and overall DevSecOps maturity;
- Strengthening cybersecurity and application security, improve security architecture, and accessibility compliance;
- Improving documentation quality, standardization, knowledge sharing, operational maturity, and long-term maintainability;

- Increasing automation and simplifying business processes and technical solutions;
- Reducing technical debt;
- Modernizing technologies;
- Enhancing user experience; and
- Improving the overall quality, maintainability, operational efficiency, and long-term maturity of the technology portfolio.

Recommendations shall be presented through the governance process established under the resulting Contract.

Managed Services include, but are not limited to, the following service areas and associated responsibilities:

4.5.1 Application Operations and Maintenance

VENDOR shall provide comprehensive Application Operations and Maintenance services necessary to ensure the continued availability, reliability, performance, security, resiliency, and operational stability of **CUSTOMER's** College and Career Advising technology portfolio.

VENDOR shall proactively monitor, administer, maintain, troubleshoot, support, and continuously improve the production environment while minimizing service disruptions, operational risk, and technical debt.

Managed Services for Application Operations and Maintenance include, but are not limited to, the following responsibilities:

- Monitoring the health, availability, performance, observability, and operational status of applications, integrations, databases, APIs, cloud services, and supporting infrastructure.
- Responding to, diagnosing, and resolving production incidents, application defects, system failures, service interruptions, and operational issues in accordance with the Service Level Agreements established under this Contract.
- Performing root cause analysis for significant production incidents and documenting corrective actions, preventive actions, and lessons learned to reduce the likelihood of recurrence.
- Performing corrective, adaptive, preventive, and perfective maintenance activities necessary to maintain a stable, secure, reliable, and supportable application environment.

- Identifying, tracking, prioritizing, and resolving software defects, operational issues, and technical debt through an established defect management process.
- Monitoring application performance and proactively recommending improvements to increase reliability, scalability, maintainability, resiliency, operational efficiency, and customer experience.
- Performing routine application administration, configuration management, environment management, and scheduled maintenance activities.
- Supporting production releases, hotfixes, emergency changes, and planned maintenance activities in accordance with the Release Management processes established under this Contract.
- Maintaining operational documentation, support procedures, system runbooks, knowledge articles, and other operational artifacts necessary to support ongoing operations and continuity of service.
- Coordinating with **CUSTOMER** and third-party vendors, as necessary, to resolve incidents, infrastructure issues, security events, integration failures, and other operational concerns affecting the technology portfolio.

VENDOR shall maintain sufficient operational support capabilities to respond to planned work, production incidents, emergency situations, legislative priorities, and other operational needs while minimizing disruption to **CUSTOMER** business operations.

VENDOR shall proactively analyze operational metrics, recurring incidents, technical debt, performance trends, capacity constraints, and support patterns for operational improvement. Recommendations shall be presented through the governance process established under the resulting Contract and shall include proposed corrective actions, anticipated benefits, implementation considerations, and any operational impacts.

4.5.2 Application Development and Enhancement

VENDOR shall provide comprehensive Application Development and Enhancement services supporting the ongoing evolution of **CUSTOMER**'s College and Career Advising technology portfolio.

Managed Services for Application Development and Enhancement include, but are not limited to, the following responsibilities:

- Designing, developing, testing, deploying, and supporting new application functionality, business capabilities, and digital services.
- Implementing enhancements, configuration changes, workflow improvements, and user experience (UX/UI) improvements across the technology portfolio.
- Modernizing existing applications, technologies, frameworks, libraries, and supporting components to improve maintainability, security, performance, scalability, operational efficiency, and long-term sustainability.
- Designing technical solutions, application architectures, database structures, integration patterns, and supporting technical components that align with **CUSTOMER's** enterprise architecture principles, technology standards, and long-term strategic objectives.
- Developing, maintaining, and enhancing RESTful APIs, web services, enterprise integrations, event-driven architectures, and data exchange processes supporting internal and external systems.
- Designing, developing, configuring, and supporting Salesforce applications, workflows, automations, integrations, and related platform capabilities.
- Developing and maintaining cloud-native applications and services utilizing Microsoft Azure and other cloud technologies adopted by **CUSTOMER**.
- Designing, developing, and maintaining database structures, data integrations, reporting solutions, data migration processes, and other data management components necessary to support application functionality.
- Developing responsive, accessible, and user-centered interfaces that comply with applicable accessibility standards and provide consistent user experiences across supported platforms.
- Refactoring existing application components to improve maintainability, reduce technical debt, simplify future enhancements, improve long-term supportability, and strengthen application resilience.
- Performing peer code reviews, adhering to established coding standards, and applying other engineering quality practices to

improve code quality, maintainability, security, consistency, and long-term supportability before software is promoted through the deployment pipeline.

- Developing reusable components, shared services, APIs, libraries, and frameworks that promote consistency, reduce duplication, simplify future development, and improve engineering efficiency across the technology portfolio.
- Performing technical impact analysis for proposed enhancements, architectural changes, technology upgrades, framework updates, and new functionality to identify potential impacts to existing applications, integrations, APIs, databases, security controls, business processes, reporting, accessibility, user experience, and operational support. **VENDOR** shall identify risks, dependencies, mitigation strategies, and recommended design modifications prior to implementation.
- Maintaining source code repositories, configuration files, deployment artifacts, technical documentation, and other software assets necessary to support the complete software development lifecycle.

VENDOR shall ensure that all application development activities are performed in accordance with the engineering standards, architectural principles, secure software development practices, Quality Engineering processes, accessibility requirements, and Release Management procedures established under this Contract.

4.5.3 Solution Architecture and Technical Design

VENDOR shall provide comprehensive Solution Architecture and Technical Design services supporting the ongoing evolution of **CUSTOMER's** College and Career Advising technology portfolio. **VENDOR** shall design technical solutions that are secure, scalable, maintainable, accessible, resilient, performant, supportable, and aligned with **CUSTOMER's** enterprise architecture principles, technology standards, and long-term strategic objectives.

Managed Services for Solution Architecture and Technical Design include, but are not limited to, the following responsibilities:

- Designing application architectures that support scalability, maintainability, resiliency, performance, security, accessibility, and long-term sustainability.

- Developing technical solution designs for new features, enhancements, modernization initiatives, integrations, APIs, cloud services, databases, and supporting infrastructure.
- Designing database schemas, data models, data integration strategies, and data management solutions that support application performance, reporting, scalability, and long-term maintainability.
- Designing and documenting RESTful APIs, integration patterns, messaging architectures, authentication mechanisms, and other shared technical services.
- Evaluating architectural alternatives and recommending technologies, frameworks, cloud services, implementation approaches, engineering patterns, and build-versus-buy alternatives that best support **CUSTOMER's** business objectives and long-term technology strategy.
- Identifying opportunities to reduce technical debt through architectural improvements, refactoring, modernization, and standardization initiatives.
- Ensuring architectural decisions consider operational supportability, cybersecurity, accessibility, disaster recovery, business continuity, monitoring, observability, and long-term lifecycle management.
- Maintaining current architecture diagrams, technical design documentation, interface specifications, database documentation, and other architectural artifacts necessary to support ongoing operations and future development.
- Participating in architecture reviews, technical planning sessions, and design discussions with **CUSTOMER** and other stakeholders.

For significant enhancements, modernization initiatives, infrastructure changes, database modifications, integration changes, API development, authentication changes, or other architectural changes identified by **CUSTOMER**, **VENDOR** shall prepare and present a **Technical Design Package** (TDP) for **CUSTOMER** review prior to implementation. At a minimum, the TDP shall include:

- Business and technical objectives
- Proposed solution architecture
- Estimated implementation effort and delivery considerations

- Architecture diagrams
- Database architecture, schema design, data model changes, and data migration considerations
- Integration and API impacts
- Security considerations
- Accessibility considerations
- Performance and scalability considerations
- Operational support considerations
- Risks, assumptions, and dependencies
- Testing strategy
- Deployment approach
- Rollback strategy
- Documentation updates

CUSTOMER shall review major architectural decisions through an Architecture Review process, prior to implementation, to ensure alignment with enterprise architecture standards, cybersecurity requirements, data governance, accessibility requirements, strategic direction, and long-term supportability. **CUSTOMER** participation in architectural reviews, technical design discussions, or solution planning activities is advisory in nature and shall not transfer responsibility for the technical quality, completeness, maintainability, security, performance, or successful implementation of the solution. **VENDOR** shall remain fully responsible for all architectural decisions, technical designs, engineering recommendations, and delivered solutions under this Contract.

VENDOR shall document significant architectural decisions through Architecture Decision Records (ADRs), or an equivalent methodology approved by **CUSTOMER**. ADRs shall document the architectural decision, alternatives considered, rationale, assumptions, dependencies, risks, and operational impacts to support long-term knowledge management, solution maintainability, and future architectural planning.

4.5.4 Quality Engineering

VENDOR shall provide comprehensive Quality Engineering services to ensure that all software developed, maintained, enhanced, or deployed under this Contract meets **CUSTOMER**'s requirements for functionality, reliability, security, accessibility, maintainability, and overall software quality. **VENDOR** shall be solely responsible for planning, executing, documenting, and continuously improving all quality assurance and testing activities necessary to validate the completeness and quality of the delivered solution.

CUSTOMER expects quality to be integrated throughout the software development lifecycle rather than performed as a discrete activity immediately prior to release. **VENDOR** shall implement mature Quality Engineering practices that emphasize defect prevention, automation, continuous testing, and continuous improvement.

Managed Services for Quality Engineering include, but are not limited to, the following responsibilities:

- Developing and maintaining a comprehensive Quality Management Plan governing testing activities throughout the software development lifecycle.
- Developing, maintaining, and executing test strategies, test plans, test cases, and test scripts appropriate for each enhancement, release, or maintenance activity.
- Performing unit testing, integration testing, system testing, end-to-end testing, user acceptance testing support, regression testing, smoke testing, and production validation testing, as appropriate.
- Developing and maintaining automated testing capabilities to improve software quality, increase testing coverage, reduce manual testing effort, and support Continuous Integration and Continuous Deployment (CI/CD) practices.
- Performing comprehensive regression testing for every production release to validate that new functionality does not adversely impact existing application functionality, integrations, APIs, databases, authentication services, reporting, or other components of the technology portfolio.
- Establishing and maintaining test data management practices, including the creation, protection, refresh, masking, and

maintenance of representative test data necessary to support reliable, repeatable, and secure testing activities.

- Performing accessibility testing to verify compliance with applicable federal and State of Texas accessibility requirements, including Web Content Accessibility Guidelines (WCAG) Version 2.1, Level AA (or successor standard), Section 508, and applicable Texas Administrative Code requirements.
- Performing application security testing appropriate to the technologies supporting **CUSTOMER**'s environment, including, where applicable, Static Application Security Testing, Dynamic Application Security Testing, software composition analysis (dependency analysis), vulnerability scanning, and remediation validation.
- Performing performance, load, scalability, and resilience testing, where appropriate, to validate application performance under anticipated operating conditions.
- Conducting peer code reviews, static code analysis, and other engineering quality practices prior to promoting software through the deployment pipeline.
- Establishing and monitoring quality metrics, including automated test coverage, defect escape rate, regression testing coverage, defect aging, production defect trends, code quality metrics, and other engineering quality indicators approved by **CUSTOMER**.
- Maintaining test results, quality metrics, defect tracking, testing documentation, and other quality artifacts necessary to demonstrate compliance with this Contract.

VENDOR shall establish, maintain, and continuously expand automated testing capabilities appropriate for the technology portfolio, to improve regression testing coverage, release quality, engineering efficiency, and overall software reliability.

VENDOR shall establish release readiness criteria and maintain a documented Definition of Done applicable to all development activities performed under this Contract. At a minimum, the **Definition of Done** shall include successful completion of required testing activities, peer code reviews, security validation, accessibility validation, documentation updates, deployment readiness verification, and any additional quality criteria established through the governance process. Software shall not be promoted to

production until all Definition of Done criteria have been successfully satisfied or formally approved through the governance process.

VENDOR shall be responsible for validating the quality and release readiness of all software prior to deployment into production. **CUSTOMER** participation in User Acceptance Testing (UAT), Sprint Reviews, demonstrations, or other quality validation activities is intended to confirm that delivered functionality satisfies business requirements and shall not transfer responsibility for software quality, testing completeness, accessibility compliance, cybersecurity, or overall release readiness to **CUSTOMER**.

VENDOR shall proactively identify recurring defects, testing gaps, and quality trends through the governance process established under the resulting Contract. Quality Engineering practices shall be continuously refined throughout the Contract term to improve software quality, reduce production defects, strengthen engineering maturity, and improve the overall reliability and maintainability of **CUSTOMER**'s technology portfolio.

4.5.5 DevSecOps and Release Management

VENDOR shall provide comprehensive DevSecOps and Release Management services supporting the secure, reliable, and efficient delivery of software changes throughout the software development lifecycle. **VENDOR** shall establish and maintain mature Continuous Integration and Continuous Deployment (CI/CD) practices that automate software builds, testing, security validation, deployment, monitoring, and operational verification while minimizing deployment risk, reducing manual effort, and improving software quality.

Managed Services for DevSecOps and Release Management include, but are not limited to, the following responsibilities:

- Designing, implementing, maintaining, and continuously improving CI/CD pipelines supporting application development, testing, deployment, security validation, and operational monitoring.
- Automating build, deployment, configuration management, infrastructure provisioning, testing, security validation, and release processes where practical.
- Maintaining version control strategies, branch management practices, source code promotion controls, and configuration management processes necessary to ensure the integrity,

traceability, reproducibility, and auditability of software releases throughout the software development lifecycle.

- Integrating security throughout the software development lifecycle by incorporating automated security scanning, dependency management, vulnerability detection, secrets management, infrastructure security validation, and other secure software development practices into the CI/CD pipeline.
- Establishing standardized deployment procedures that promote consistency, repeatability, traceability, operational reliability, and auditability.
- Developing, maintaining, and executing Release Plans, deployment plans, implementation schedules, rollback plans, and release documentation for all production releases.
- Coordinating release activities across applications, integrations, cloud services, databases, infrastructure, and third-party platforms to minimize operational risk and service disruption.
- Performing deployment validation, smoke testing, operational verification, production health checks, and post-deployment monitoring immediately following each production deployment.
- Monitoring production deployments to identify and resolve deployment-related issues, performance degradation, security concerns, or operational impacts.
- Maintaining release records, deployment documentation, configuration baselines, deployment histories, and other operational artifacts necessary to support auditability, operational support, and future maintenance.
- Continuously improving deployment automation, release processes, DevSecOps practices, and operational procedures to improve software quality, reduce deployment risk, increase deployment frequency, and improve operational resilience.

VENDOR shall utilize deployment strategies that minimize service disruption and operational risk. Blue/Green Deployments, Canary Releases, Rolling Deployments, or other deployment methodologies that provide seamless production cutover, production validation, and rapid rollback capability are encouraged where technically appropriate.

VENDOR shall recommend and implement deployment strategies that best support application availability, operational stability,

business continuity, efficient recovery from deployment failures, and the operational characteristics of the technologies comprising **CUSTOMER**'s environment.

For every production release, **VENDOR** shall develop and execute a documented Release Plan that includes, at a minimum:

- Release scope and objectives
- Deployment activities and sequencing
- Pre-deployment validation activities
- Production smoke testing procedures
- Post-deployment operational verification
- Rollback procedures
- Success criteria
- Communications plan
- Roles and responsibilities
- Known risks, assumptions, and mitigation strategies

Prior to each production deployment, **VENDOR** shall complete a **Release Readiness Assessment (RRA)** documenting all Definition of Done criteria, required testing activities, security validation, accessibility validation, deployment prerequisites, rollback procedures, production support preparations, operational readiness activities, and other release requirements have been successfully completed.

Operational readiness shall include, at a minimum, confirmation that:

- Support teams have been notified of the planned release.
- Operational runbooks and technical documentation have been updated.
- Monitoring, logging, and alerting capabilities have been configured or validated.
- Deployment documentation has been completed and verified.
- On-call support personnel and escalation procedures have been established, where applicable.

VENDOR shall validate that all release readiness requirements and Definition of Done criteria have been satisfied prior to deployment into production. **VENDOR** shall remain fully responsible for the

successful execution of all production deployments, deployment verification activities, rollback decisions, production validation, and operational stabilization following each release.

The RRA shall be made available to **CUSTOMER** upon request and shall serve as **VENDOR**'s formal confirmation that the release is ready for production deployment.

CUSTOMER participation in release planning, deployment reviews, production validation activities, or release approvals shall not transfer responsibility for deployment quality, release execution, production stability, operational readiness, or the successful implementation of a production release to **CUSTOMER**.

4.5.6 Cloud Operations and Infrastructure

VENDOR shall provide comprehensive Cloud Operations and Infrastructure services necessary to support the reliable, secure, resilient, and efficient operation of **CUSTOMER**'s cloud-hosted applications and supporting technology platforms. **VENDOR** shall manage and support cloud resources within the scope of this Contract while collaborating with **CUSTOMER** on enterprise cloud governance, networking, identity management, cybersecurity, and other shared technology services.

Managed Services for Cloud Operations and Infrastructure include, but are not limited to, the following responsibilities:

- Administering and supporting Microsoft Azure resources supporting **CUSTOMER**'s application portfolio.
- Configuring, maintaining, and optimizing cloud services, application environments, platform services, storage, databases, networking components, and other cloud resources supporting the managed applications.
- Monitoring application availability, resource utilization, system health, performance, capacity, and operational status across cloud-hosted environments.
- Implementing and maintaining centralized logging, telemetry, monitoring, alerting, dashboards, and operational reporting necessary to support proactive operations, performance management, and incident response.
- Managing application configuration, environment configuration, application settings, configuration baselines, and environment

consistency across Development, Test, Quality Assurance, Staging, and Production environments.

- Supporting Infrastructure as Code (IaC), configuration automation, and environment provisioning to improve consistency, repeatability, scalability, and operational efficiency.
- Continuously monitoring cloud resource consumption and utilization and proactively recommending opportunities to optimize application performance, improve operational efficiency, right-size cloud resources, eliminate underutilized or orphaned cloud resources, and reduce unnecessary cloud costs while maintaining required service levels and application availability.
- Supporting application backup, recovery, disaster recovery, high availability, business continuity, and resiliency capabilities appropriate to the technology portfolio.
- Coordinating cloud infrastructure changes, application deployments, maintenance activities, and operational support with **CUSTOMER** and other service providers, as necessary.
- Maintaining cloud architecture documentation, configuration documentation, operational procedures, environment inventories, and other infrastructure artifacts necessary to support ongoing operations and long-term maintainability.

VENDOR shall continuously monitor the health and operational performance of the supported environments and proactively identify risks, performance bottlenecks, capacity constraints, configuration issues, cybersecurity concerns, and other operational conditions that could negatively impact application availability, reliability, or service delivery.

CUSTOMER retains responsibility for enterprise cloud governance, tenant administration, enterprise networking, identity services, enterprise cybersecurity policies, and other shared technology services not expressly assigned to **VENDOR** under this Contract.

VENDOR shall coordinate with **CUSTOMER** to support these shared responsibilities while remaining fully responsible for the operation, configuration, performance, reliability, security, resiliency, and supportability of the cloud resources and application environments within the scope of this Contract.

4.5.7 Security and Compliance

VENDOR shall provide comprehensive information security, cybersecurity, and compliance services necessary to protect the confidentiality, integrity, availability, and resilience of **CUSTOMER**'s managed application portfolio and **CUSTOMER** Data. Security shall be integrated throughout the software development lifecycle, application operations, and supporting engineering practices using a secure-by-design and DevSecOps approach.

Managed Services for Security and Compliance include, but are not limited to, the following responsibilities:

- Designing, developing, configuring, and maintaining applications in accordance with secure software engineering principles and industry-recognized cybersecurity best practices.
- Implementing and maintaining appropriate application security controls, authentication mechanisms, authorization controls, encryption, logging, auditing, and secure configuration practices.
- Managing application secrets, certificates, encryption keys, service accounts, API credentials, and other sensitive configuration information using secure storage, rotation, monitoring, and access management practices appropriate to the technologies supporting **CUSTOMER**'s environment.
- Monitoring, identifying, documenting, prioritizing, and remediating application security vulnerabilities within timeframes established by **CUSTOMER**'s security policies and governance processes.
- Applying security patches, software updates, framework updates, and other vendor-released security remediations in accordance with **CUSTOMER** security policies, vendor guidance, risk assessments, and approved maintenance windows.
- Conducting periodic security configuration reviews of applications, cloud resources, APIs, databases, integrations, and supporting components to verify continued compliance with **CUSTOMER** security standards, identify configuration drift, validate secure baseline configurations, and recommend corrective actions.
- Supporting vulnerability assessments, penetration testing, security reviews, audits, and other security assessment activities

requested by **CUSTOMER** or required by applicable laws, regulations, or policies.

- Maintaining application dependencies, third-party libraries, frameworks, and open-source components in supported versions and promptly addressing known security vulnerabilities.
- Supporting compliance with applicable State of Texas cybersecurity requirements, including Tex. Admin. Code Chapter 477, the Texas Cybersecurity Framework, Texas Risk and Authorization Management Program (TX-RAMP) requirements when applicable, and **CUSTOMER** information security policies, standards, and procedures.
- Supporting security incident response activities by providing technical resources, system information, log data, forensic support, root cause analysis, and corrective action plans, as requested by **CUSTOMER**.
- Maintaining audit logs, security documentation, configuration baselines, and other security artifacts necessary to demonstrate compliance with applicable security requirements.
- Supporting identity and access management controls within the managed applications while coordinating with **CUSTOMER** regarding enterprise identity services.
- Protecting **CUSTOMER** Confidential Information and other sensitive information from unauthorized access, disclosure, alteration, destruction, loss, or inappropriate use throughout its lifecycle.

VENDOR shall promptly notify **CUSTOMER** of any actual or suspected security incident, unauthorized access, vulnerability, compromise, or other cybersecurity event affecting the applications, environments, or services within the scope of this Contract in accordance with **CUSTOMER** security policies, incident response procedures, and applicable reporting requirements.

CUSTOMER retains responsibility for enterprise cybersecurity governance, enterprise security operations, security policy development, risk management, compliance oversight, and other enterprise security functions not expressly assigned to **VENDOR** under this Contract. **VENDOR** shall coordinate with **CUSTOMER** to support these shared responsibilities while remaining fully responsible for the security, integrity, resilience, and supportability of

the applications, application environments, and services within the scope of this Contract.

4.5.8 Documentation and Knowledge Management

VENDOR shall provide comprehensive Documentation and Knowledge Management services to ensure that **CUSTOMER** maintains complete, accurate, current, and accessible technical documentation supporting the ongoing operation, maintenance, enhancement, governance, and future modernization of the College and Career Advising technology portfolio.

Managed Services for Documentation and Knowledge Management include, but are not limited to, the following responsibilities:

- Developing, maintaining, and updating system architecture documentation, solution architecture diagrams, infrastructure diagrams, network diagrams, integration diagrams, application dependency documentation, and other architectural artifacts.
- Maintaining TDPs, ADRs, Release Plans, RRAs, and other engineering artifacts established under this Contract.
- Developing and maintaining database documentation, including logical and physical data models, database schemas, data dictionaries, entity relationship diagrams, data flows, and other database design documentation.
- Maintaining API documentation, interface specifications, integration documentation, message formats, authentication methods, and other technical interface documentation.
- Maintaining operational documentation, including standard operating procedures, production support procedures, deployment procedures, configuration documentation, runbooks, recovery procedures, troubleshooting guides, and operational playbooks.
- Maintaining cloud architecture documentation, IaC repositories, environment inventories, configuration baselines, and environment-specific documentation.
- Maintaining technical documentation for application configuration, security controls, monitoring, alerting, logging, and operational support activities.
- Developing and maintaining user documentation, administrator guides, technical reference materials, and other documentation

necessary to support the operation, maintenance, and administration of the technology portfolio.

- Ensuring documentation is version controlled, readily accessible, and maintained within **CUSTOMER**-approved repositories and knowledge management platforms.
- Maintaining all technical documentation, operational procedures, architecture artifacts, runbooks, knowledge articles, and other engineering documentation within **CUSTOMER**-approved knowledge management repositories to ensure documentation remains current, searchable, accessible, and available to **CUSTOMER** personnel throughout the Contract term.
- Periodically reviewing technical documentation, operational procedures, runbooks, architecture artifacts, and knowledge articles to verify they remain accurate, complete, current, and aligned with the production environment, and promptly correcting identified deficiencies.
- Supporting knowledge transfer activities throughout the Contract term, including onboarding, cross-training, operational handoffs, transition planning, and Contract transition activities.

VENDOR shall update applicable documentation as part of every approved enhancement, maintenance activity, architectural change, production release, configuration change, operational improvement, or other material modification to the technology portfolio.

Documentation shall be maintained as a living operational asset throughout the Contract term and shall be considered a required deliverable under the Definition of Done.

Documentation shall be completed and stored within **CUSTOMER**-approved repositories prior to production deployment unless otherwise approved by **CUSTOMER**.

VENDOR shall conduct periodic knowledge transfer sessions with **CUSTOMER** personnel covering application architecture, operational procedures, cloud environments, cybersecurity, deployment processes, significant enhancements, and other technical topics requested by **CUSTOMER**.

Knowledge transfer shall be an ongoing responsibility throughout the Contract term and shall not be limited to Contract transition activities.

All documentation, architecture artifacts, operational procedures, technical specifications, engineering artifacts, and knowledge assets produced under this Contract shall become the property of **CUSTOMER** and shall be maintained in formats that support long-term maintenance, operational continuity, knowledge transfer, and transition to **CUSTOMER** personnel or a successor **VENDOR**.

VENDOR shall maintain documentation at a level of detail sufficient to enable **CUSTOMER** or a successor **VENDOR** to successfully operate, support, maintain, and enhance the technology portfolio without unreasonable dependence upon individual **VENDOR** personnel.

4.5.9 Agile Delivery Management

VENDOR shall utilize Agile software delivery methodologies to plan, develop, test, deploy, and continuously improve **CUSTOMER**'s technology portfolio. Agile delivery practices shall promote collaboration, transparency, predictable delivery, continuous feedback, and rapid delivery of business value while maintaining the engineering, quality, cybersecurity, and governance standards established under this Contract.

CUSTOMER shall establish business priorities, maintain ownership of the product vision and product backlog, define business requirements, establish feature priorities, and accept completed work. **CUSTOMER** will designate one or more Product Owners responsible for representing business priorities and providing direction regarding product functionality and backlog prioritization.

VENDOR shall provide experienced Agile delivery leadership, including Scrum Masters or other Agile facilitators, Delivery Managers, Engineering Leads, Technical Architects, Quality Engineering personnel, and other resources necessary to successfully execute Agile software delivery. **VENDOR** shall remain responsible for sprint planning, technical design, estimation, engineering execution, quality, release readiness, and successful delivery of all work performed under this Contract.

VENDOR shall organize its personnel into one or more Agile delivery teams capable of supporting application operations, maintenance, modernization, and new feature development across **CUSTOMER**'s technology portfolio.

VENDOR may propose the composition, structure, and Agile delivery methodology of its delivery teams, provided the proposed approach

satisfies the requirements of this Contract, aligns with industry best practices, and supports the **CUSTOMER**'s business priorities.

Managed Services for Agile Delivery Management include, but are not limited to, the following Agile delivery activities:

- Product Backlog Refinement
- Sprint Planning (or equivalent iteration planning activities)
- Daily Team Synchronization Meetings (Daily Scrum or equivalent)
- Sprint Reviews
- Sprint Retrospectives
- Release Planning
- Sprint Demonstrations
- Estimation and Capacity Planning
- Dependency Management
- Technical Design Reviews
- Backlog Grooming
- Production Release Planning
- Maintaining and reporting Agile delivery metrics, including sprint predictability, delivery throughput, backlog health, work item aging, and other metrics approved through the governance process to support delivery transparency and continuous improvement.

VENDOR shall collaborate with the **CUSTOMER** to establish sprint goals, release objectives, delivery commitments, and resource capacity appropriate to **CUSTOMER**'s priorities and available funding. Sprint commitments shall reflect realistic team capacity while maintaining flexibility to address production support activities, legislative priorities, security vulnerabilities, emergency work, and other **CUSTOMER**-directed priorities.

CUSTOMER may reprioritize work throughout the Contract term based upon changing business needs, legislative requirements, production incidents, cybersecurity risks, funding, or other operational considerations. **VENDOR** shall work collaboratively with **CUSTOMER** to evaluate impacts to sprint commitments, release schedules, staffing, and delivery plans resulting from changes in priorities.

VENDOR shall support quarterly delivery planning activities with CUSTOMER to review product roadmaps, technology roadmaps, anticipated initiatives, resource capacity, architectural dependencies, release planning, modernization opportunities, and other strategic considerations. Quarterly planning is intended to improve delivery predictability and long-term planning and shall not limit **CUSTOMER's** ability to reprioritize work as business needs evolve.

VENDOR shall ensure that all work performed under this Contract complies with the Definition of Done, TDPs, Architecture Review requirements, Quality Engineering practices, DevSecOps processes, Release Management procedures, Documentation and Knowledge Management requirements, and all other engineering standards established under this RFO.

4.5.10 Continuous Improvement and Innovation

VENDOR shall actively promote a culture of continuous improvement, engineering excellence, and innovation throughout the Contract term.

Continuous Improvement and Innovation activities shall include, at a minimum, the following:

- Identifying opportunities to modernize applications, frameworks, libraries, platforms, and supporting technologies.
- Recommending architectural improvements that improve scalability, maintainability, resiliency, security, and operational supportability.
- Identifying opportunities to reduce technical debt, simplify application designs, eliminate unnecessary complexity, and standardize engineering practices.
- Recommending automation opportunities across software development, testing, deployments, cloud operations, monitoring, documentation, and operational support.
- Identifying opportunities to improve application performance, scalability, reliability, accessibility, usability, and customer experience.
- Recommending improvements to cloud architecture, cloud resource utilization, operational efficiency, and cost optimization.

- Evaluating emerging technologies, engineering practices, cloud services, AI-assisted development capabilities, and other innovations that may provide measurable value to **CUSTOMER**.
- Recommending improvements to Quality Engineering, DevSecOps, cybersecurity, release management, documentation, knowledge management, and operational processes.
- Identifying recurring operational issues, production trends, support patterns, and engineering opportunities through analysis of incidents, defects, performance metrics, and operational data.
- Developing recommendations that support the long-term modernization and sustainability of **CUSTOMER**'s technology portfolio.

CUSTOMER encourages **VENDOR** to responsibly evaluate and leverage emerging technologies, including artificial intelligence, machine learning, intelligent automation, and other engineering productivity tools where they provide measurable value to **CUSTOMER**. **VENDOR**'s use of emerging technologies shall remain consistent with applicable laws, regulations, **CUSTOMER** policies, cybersecurity requirements, and contractual obligations.

VENDOR shall periodically present Continuous Improvement recommendations through the governance process established under this Contract. Recommendations shall include business value, technical rationale, anticipated benefits, estimated effort, dependencies, risks, implementation considerations, and any operational impacts associated with each recommendation.

Submission of recommendations does not obligate **CUSTOMER** to authorize implementation. No improvement initiative shall be implemented without **CUSTOMER** approval through the governance processes established under this Contract.

4.6 Governance

CUSTOMER and **VENDOR** shall establish and maintain a collaborative governance framework that promotes transparency, strategic alignment, accountability, effective decision-making, proactive risk management, continuous improvement, and successful delivery of Managed Services throughout the Contract term.

The governance framework shall provide structured oversight of application operations, project delivery, architecture, cloud services, cybersecurity, Quality Engineering, release management, staffing, financial management,

risks, issues, performance, service levels, and continuous improvement. Governance shall ensure that business priorities remain aligned with technical execution while enabling timely decisions, effective communication, proactive issue resolution, and ongoing collaboration between **CUSTOMER** and **VENDOR**.

Governance shall emphasize timely decision-making at the appropriate level of the organization while providing clear escalation paths for strategic, financial, contractual, architectural, cybersecurity, or enterprise-impacting decisions requiring executive review.

Within thirty (30) calendar days after Contract execution, **VENDOR** shall submit a Governance Plan for **CUSTOMER** approval. The Governance Plan shall define roles, delegated decision authority, materiality thresholds, meeting cadence, escalation paths, required artifacts, and target decision timeframes.

CUSTOMER shall establish business priorities, approve funding, define product direction, approve major deliverables, and provide overall contract oversight. **CUSTOMER** may designate employees, contractors, or other authorized representatives to participate in governance activities, architecture reviews, quality reviews, technical assessments, acceptance activities, or other oversight functions performed under this Contract. Participation by **CUSTOMER**-designated representatives shall constitute participation by the **CUSTOMER** for purposes of this Contract.

VENDOR shall remain responsible for planning, managing, staffing, engineering, delivering, operating, supporting, securing, and continuously improving all services provided under this Contract. Governance activities, **CUSTOMER** participation in reviews or approvals, and **CUSTOMER** oversight shall not relieve the **VENDOR** of responsibility for the quality, completeness, security, performance, maintainability, operational stability, or successful delivery of the services provided under this Contract.

CUSTOMER intends to evaluate **VENDOR** based upon delivery outcomes, engineering quality, operational performance, customer satisfaction, service level achievement, continuous improvement, innovation, and the overall value delivered rather than solely upon resource utilization or hours worked.

4.6.1 Governance Model

The governance framework shall include multiple levels of oversight to support strategic direction, operational management, software delivery, technical decision-making, and continuous improvement throughout the Contract term. Governance activities shall be structured to ensure that decisions are made at the appropriate level

of the organization while providing clear escalation paths for matters requiring executive review or **CUSTOMER** approval.

At a minimum, the governance framework shall include the following governance functions:

- **Executive Governance**

Executive Governance shall provide strategic oversight of the engagement and focus on overall Contract performance, business priorities, financial management, organizational alignment, strategic initiatives, major risks, significant issues, continuous improvement opportunities, and long-term planning.

- **Operational Governance**

Operational Governance shall oversee the day-to-day delivery of Managed Services, including application operations, service performance, cloud operations, cybersecurity, Quality Engineering, release management, staffing, service levels, operational metrics, risks, issues, and other matters affecting the ongoing operation of the technology portfolio.

- **Delivery Governance**

Delivery Governance shall support Agile software delivery by overseeing product backlogs, sprint planning, delivery commitments, release planning, technical dependencies, resource planning, delivery risks, and coordination across **CUSTOMER**'s technology portfolio to ensure business priorities remain aligned with engineering execution.

- **Technical Governance**

Technical Governance shall provide oversight of solution architecture, TDPs, ADRs, cloud architecture, cybersecurity, engineering standards, technology standards, technical debt, modernization initiatives, and other significant technical decisions requiring **CUSTOMER** review or governance.

The governance framework shall remain sufficiently flexible to accommodate the evolving needs of the engagement. Governance activities may be combined, modified, or supplemented throughout the Contract term by mutual agreement of **CUSTOMER** and **VENDOR**, provided the governance objectives established under this Contract continue to be satisfied.

VENDOR shall actively participate in governance activities requested by **CUSTOMER** and shall provide personnel possessing the appropriate authority, technical expertise, and decision-making responsibility necessary to support effective governance and timely resolution of issues. Participants may include executive leadership, Engagement Managers, Delivery Managers, Scrum Masters, Technical Architects, Engineering Leads, Product Owners, Quality Engineering Leads, Cloud Engineers, cybersecurity personnel, and other subject matter experts, as appropriate.

VENDOR shall maintain governance artifacts necessary to support effective management of the engagement, including governance calendars, decision logs, action item registers, risk registers, issue logs, meeting minutes, status reports, and other documentation necessary to support governance activities.

4.6.2 Governance Meetings and Communication

CUSTOMER and **VENDOR** shall maintain regular governance meetings and other collaborative working sessions necessary to support the governance framework established under this Contract. Governance meetings are intended to facilitate strategic planning, operational coordination, software delivery, technical decision-making, performance management, risk management, issue resolution, and continuous improvement throughout the Contract term. Governance activities shall promote timely communication, collaborative decision-making, transparency, and alignment between business priorities and technical execution.

Unless otherwise approved by **CUSTOMER**, **VENDOR** shall prepare meeting agendas, supporting materials, meeting minutes, action item registers, and follow-up activities for governance meetings within the scope of this Contract. Governance artifacts shall be maintained as part of the Contract documentation and made available to **CUSTOMER** upon request.

At a minimum, the governance framework shall include the following recurring governance meetings:

- **Executive Governance Meetings**

Executive Governance Meetings shall provide executive oversight of Contract performance, strategic initiatives, business priorities, financial management, organizational alignment, major risks, significant issues, technology roadmaps, modernization initiatives, and opportunities for continuous improvement.

- **Operational Governance Meetings**

Operational Governance Meetings shall focus on the ongoing delivery of Managed Services, including operational performance, service levels, staffing, incidents, problems, cloud operations, cybersecurity, application health, Quality Engineering metrics, release activities, risks, issues, action items, and overall operational performance.

- **Delivery Governance Meetings**

Delivery Governance Meetings shall support Agile software delivery and product execution through Sprint Planning, Sprint Reviews, Sprint Retrospectives, Product Backlog Refinement, Release Planning, dependency management, delivery commitments, and other collaborative activities necessary to successfully deliver the software development lifecycle.

- **Technical Governance Meetings**

Technical Governance Meetings shall review TDPs, ADRs, solution architecture, cloud architecture, cybersecurity considerations, modernization initiatives, significant technical decisions, engineering standards, technical debt, and other technical matters requiring **CUSTOMER** review or governance.

CUSTOMER may establish additional governance meetings throughout the Contract term to address emerging business priorities, legislative initiatives, technology modernization efforts, cybersecurity matters, operational issues, or other business needs. Governance meetings may be modified in frequency, combined, or supplemented as the needs of the engagement evolve.

VENDOR shall ensure that meeting participants possess the appropriate authority, technical expertise, and decision-making responsibility necessary to support productive governance discussions, timely decisions, and effective resolution of action items.

Meeting outcomes shall be documented through meeting minutes, decision logs, action item registers, risk registers, issue logs, status reports, and other governance artifacts, as appropriate. **VENDOR** shall maintain these artifacts throughout the Contract term and provide status updates on open action items, risks, issues, decisions, and agreed-upon follow-up activities during subsequent governance meetings.

4.6.3 Communication and Escalation

VENDOR shall maintain open, transparent, and proactive communication with **CUSTOMER** throughout the Contract term. **VENDOR** shall promptly communicate emerging risks, issues, dependencies, staffing concerns, schedule impacts, cybersecurity events, production incidents, and other matters that may materially affect the successful delivery or operation of the services provided under this Contract. **VENDOR** shall include in these communications its assessments of business and technical impacts, recommended mitigation strategies, estimated resolution timeframes, and proposed corrective actions.

VENDOR shall escalate issues in accordance with the governance framework established under this Contract and shall not delay communication while attempting to independently resolve matters that could materially affect project delivery, service availability, security, schedule, budget, or **CUSTOMER** operations.

4.7 Performance Management and Service Reporting

4.7.1 Performance Management

CUSTOMER shall evaluate **VENDOR**'s performance throughout the Contract term based upon delivery outcomes, operational performance, engineering quality, customer satisfaction, continuous improvement, compliance with Contract requirements, and achievement of agreed-upon Service Level Agreements, Key Performance Indicators, and other performance measures established under this Contract. **VENDOR** shall establish and maintain performance measurement processes that provide meaningful visibility into the health of the engagement and support data-driven decision-making.

Performance management shall promote accountability, transparency, continuous improvement, and proactive identification of risks, trends, and opportunities to improve service delivery. Performance measures are intended to evaluate the effectiveness of the Managed Services engagement rather than the productivity of individual personnel.

VENDOR shall collect, maintain, analyze, and report performance metrics necessary to evaluate delivery performance, operational effectiveness, engineering quality, service reliability, cloud operations, cybersecurity, software quality, release management,

documentation quality, knowledge management, customer satisfaction, and overall service delivery.

At a minimum, **VENDOR** shall report performance information related to the following areas:

- Application availability and operational performance.
- Incident, problem, and service request management.
- Defect trends, quality metrics, and production stability.
- Sprint delivery performance and release outcomes.
- Engineering quality and automated testing metrics.
- Cloud operations, utilization, and operational health.
- Cybersecurity performance and vulnerability remediation.
- Documentation quality, knowledge management, and completion of required engineering artifacts.
- Staffing, resource utilization, and capacity planning.
- Risks, issues, dependencies, and mitigation activities.
- Continuous improvement initiatives and modernization recommendations.
- Customer satisfaction and overall service delivery performance.

VENDOR shall identify performance trends, recurring issues, opportunities for improvement, and emerging risks through ongoing analysis of operational metrics and service delivery data. Where performance falls below established expectations or negative performance trends are identified, **VENDOR** shall provide root cause analysis, corrective action plans, implementation timeframes, and recommendations to improve future performance.

Performance measures, Key Performance Indicators, Service Level Agreements, reporting formats, reporting frequency, dashboards, and performance thresholds may be refined by mutual agreement following Contract award, provided such refinements remain consistent with the requirements of this Contract and do not materially alter the scope of services.

4.7.2 Performance Reporting

VENDOR shall prepare and deliver periodic reports supporting governance, operational oversight, performance management, and strategic planning.

At a minimum, **VENDOR** shall provide:

- Executive Performance Reports, on a schedule to be determined by the Parties upon Contract execution
- Monthly Service Performance Reports, to include the following information:
 - Sprint Status
 - Release Reports
 - Quality Engineering Reports
 - Cloud Operations Reports
 - Security and Compliance Reports
 - Risk and Issue Registers
 - Capacity Planning Reports
 - Continuous Improvements
 - Performance Dashboards

Reports shall summarize completed work, work in progress, upcoming activities, key accomplishments, risks, issues, mitigation strategies, staffing changes, engineering metrics, operational metrics, performance trends, and recommendations requiring **CUSTOMER** review or action.

CUSTOMER may request additional reports or modify reporting formats, dashboards, or reporting frequency during the Contract term to support evolving business, operational, audit, legislative, or management requirements.

4.8 Service Readiness, Transition, and Continuity

VENDOR shall provide the services necessary to support the orderly assumption, operational onboarding, ongoing operation, expansion, and eventual transition of the Managed Services described in this Contract. Service readiness and transition activities shall be planned and executed to minimize operational disruption, maintain continuity of service, preserve institutional knowledge, and reduce operational risk throughout the Contract term.

VENDOR shall cooperate fully with **CUSTOMER** and other authorized parties during all service readiness and transition activities and shall support the orderly transfer of knowledge, documentation, operational responsibilities, technical assets, engineering artifacts, and other information necessary to

ensure the continued operation, support, and long-term maintainability of **CUSTOMER's** technology portfolio.

4.8.1 Service Transition and Operational Readiness

Following Contract award, **VENDOR** shall collaborate with **CUSTOMER** to develop, maintain, and execute a Service Transition Plan appropriate to the complexity of the transition and **VENDOR's** familiarity with **CUSTOMER's** technology portfolio. The Service Transition Plan shall describe the activities necessary to successfully assume responsibility for the Managed Services described in this Contract and shall be subject to **CUSTOMER** review and approval.

The level of transition activities required shall be commensurate with the complexity of the transition and **VENDOR's** familiarity with **CUSTOMER's** environment. **CUSTOMER** may require additional transition activities where necessary to ensure operational readiness, continuity of services, successful onboarding of new resources, applications, platforms, technologies, or other changes affecting the Managed Services.

The Service Transition Plan may include, as applicable:

- Transition objectives and overall approach.
- Transition schedule and key milestones.
- Governance and communication activities.
- Knowledge transfer activities.
- Documentation review and validation.
- Technical environment assessment and validation.
- Application, infrastructure, and operational readiness assessments.
- Validation of service management processes, support responsibilities, and operational procedures.
- Access provisioning and onboarding activities.
- Resource assignments and transition responsibilities.
- Identification of transition risks, dependencies, assumptions, and mitigation strategies.
- Operational readiness criteria and transition acceptance activities.
- Success criteria for transition to steady-state operations.

VENDOR shall conduct discovery, validation, and transition activities appropriate to its familiarity with **CUSTOMER's** environment and necessary to successfully assume responsibility for the services provided under this Contract. **VENDOR** shall validate its operational readiness, including staffing, technical capabilities, documentation, operational procedures, system access, governance participation, support processes, monitoring capabilities, and other activities necessary to support successful service delivery beginning on the Contract effective date.

VENDOR shall identify documentation gaps, operational risks, technical debt, supportability concerns, or other issues identified during transition activities and present recommendations to **CUSTOMER** through the governance framework established under this Contract.

The Service Transition Plan shall be maintained throughout the transition period and updated as necessary to reflect changes in scope, schedule, risks, dependencies, or other material transition activities.

Completion of the Service Transition Plan and associated transition activities shall not relieve **VENDOR** of responsibility for successfully performing all services described in this Contract.

4.8.2 Ongoing Service Transition

During the Contract term, **CUSTOMER** may introduce additional applications, business divisions, products, platforms, technologies, integrations, cloud services, business capabilities, or other services into the scope of the Managed Services engagement. **CUSTOMER** may also undertake significant modernization initiatives, platform migrations, organizational changes, or other material changes affecting services already within the scope of this Contract.

VENDOR shall support the orderly transition of such services into the managed environment by maintaining and executing the Service Transition Plan or developing transition activities appropriate to the scope and complexity of the changes, and performing the discovery, validation, documentation, knowledge transfer, operational readiness, technical assessment, and planning activities necessary to successfully assume responsibility for ongoing support.

Transition activities shall be commensurate with the complexity, operational impact, and risk associated with the services or changes being incorporated into the engagement. **VENDOR** shall collaborate

with **CUSTOMER** to develop transition activities that minimize operational disruption, preserve institutional knowledge, maintain continuity of service, and ensure operational readiness before assuming responsibility for ongoing support.

VENDOR shall identify documentation gaps, operational risks, technical debt, supportability concerns, staffing impacts, or other issues identified during ongoing transition activities and present recommendations to **CUSTOMER** through the governance framework established under this Contract.

4.8.3 Service Transition and Contract Closeout

Upon expiration, termination, or non-renewal of the Contract, **VENDOR** shall cooperate fully with **CUSTOMER** to support an orderly transition of services to **CUSTOMER** or a successor **VENDOR** designated by **CUSTOMER**.

VENDOR shall develop, maintain, and execute a Service Transition Plan appropriate to the scope and complexity of the transition and shall coordinate all transition and contract closeout activities with **CUSTOMER**.

Transition and contract closeout activities shall be planned and executed to minimize operational disruption, preserve institutional knowledge, and ensure continuity of service throughout the transition period.

VENDOR shall provide reasonable transition assistance throughout the transition period, as directed by **CUSTOMER** and consistent with the terms of this Contract, to facilitate an orderly transfer of services and minimize disruption to **CUSTOMER** operations.

Transition activities shall include, at a minimum:

- Knowledge transfer activities.
- Delivery of all technical documentation and engineering artifacts.
- Delivery of operational documentation, runbooks, procedures, configuration documentation, and support materials.
- Transfer of source code, configuration files, deployment artifacts, IaC, automation scripts, CI/CD pipelines, and other Contract deliverables.
- Transfer of TDPs, ADRs, Release Plans, RRAs, Service Transition Plans, architecture documentation, and other engineering artifacts developed under this Contract.

- Transfer of application inventories, environment documentation, operational procedures, monitoring configurations, dashboards, and other technical assets necessary to support continued operations.
- Support for transition meetings, technical workshops, and knowledge transfer sessions with **CUSTOMER** and any successor **VENDOR**.
- Coordination of operational handoff activities, including transfer of open incidents, problems, defects, risks, issues, enhancement requests, technical debt, work in progress, and other ongoing operational activities.
- Assistance with the orderly transfer of administrative knowledge, operational responsibilities, support processes, governance artifacts, and service management processes necessary to ensure continued operation of the managed applications.

VENDOR shall continue to perform all Contract responsibilities throughout the transition period, including participation in governance activities, operational support, release activities, production operations, incident response, and other services required under this Contract, unless otherwise directed by **CUSTOMER**.

Transition activities shall not relieve **VENDOR** of its responsibility to satisfy Contract requirements, meet applicable service levels, or achieve established performance expectations until transition has been successfully completed or the Contract has otherwise concluded.

VENDOR shall not withhold documentation, source code, configuration information, technical knowledge, engineering artifacts, or other Contract deliverables pending resolution of contractual, financial, or other disputes. All work products, documentation, engineering artifacts, and deliverables developed under this Contract shall remain the property of **CUSTOMER** and shall remain available throughout the transition period to support continuity of operations and an orderly transfer of services.

4.9 Deliverables

VENDOR shall prepare, maintain, and deliver all deliverables required under this RFO as necessary to support the successful delivery, operation, governance, and continuous improvement of the Managed Services. **VENDOR** shall support engineering, operational, governance, knowledge

management, performance management, and contract administration activities throughout the Contract term.

The Deliverables Summary provided below is intended to serve as a consolidated reference to the principal deliverables required under this RFO. The summary is provided for convenience and does not modify, limit, or replace the detailed requirements established elsewhere in this RFO. Unless otherwise specified, the content, format, timing, review process, and acceptance criteria applicable to each deliverable shall be governed by the corresponding section of this RFO.

Deliverables Summary	Deadline	Responsible Party	RFO Section
Risk Register	Ongoing	VENDOR	4.6.1
Issue Log	Ongoing	VENDOR	4.6.1
Decision Log	Ongoing	VENDOR	4.6.1
Release Readiness Assessment	As needed	VENDOR	4.5.5
Service Performance Report	Monthly	VENDOR	4.7.2
Executive Report	TBD	VENDOR	4.7.2

5. Security Requirements

VENDOR shall comply with the Information Security Standards set forth in Appendix B and otherwise below, **CUSTOMER** information security policies and standards, and all other contractual security requirements applicable to the performance of this Contract.

5.1 Security Certifications and Compliance

VENDOR shall, as applicable to the services provided under this Contract:

- Maintain an appropriate TX-RAMP certification unless exempt under applicable State of Texas requirements.
- Demonstrate compliance with applicable National Institute of Standards and Technology (NIST) security and privacy controls appropriate to the systems and data supporting this engagement.
- Maintain a current SOC 2 Type II report or an equivalent independent third-party security assessment acceptable to **CUSTOMER**.
- Provide evidence of an independent penetration test performed within the preceding two (2) years and provide executive summaries or remediation status upon **CUSTOMER** request.

- Comply with 1 Tex. Admin. Code, Chapter 477, the Texas Cybersecurity Framework, Family Educational Rights and Privacy Act (FERPA), and all other applicable federal and State of Texas security and privacy requirements applicable to the services provided under this Contract.
- Comply with all applicable **CUSTOMER** information security policies, standards, procedures, and security directives.

5.2 Security Documentation

Upon request, **VENDOR** shall provide documentation reasonably necessary to support **CUSTOMER** risk management, audits, regulatory compliance, or security reviews, including:

- System Security Plans, including identified findings and planned remediation activities for Critical, High, and Moderate vulnerabilities.
- Current network architecture diagrams identifying external connections and applicable security controls.
- Data flow diagrams, where applicable.
- Security policies or other documentation reasonably necessary to demonstrate compliance with Contract requirements.

5.3 Administrative Security Requirements

VENDOR shall:

- Ensure personnel assigned to the engagement successfully complete **CUSTOMER**-approved or DIR-approved cybersecurity awareness training prior to receiving access to **CUSTOMER** systems or confidential information and provide attestation upon request.
- Ensure **CUSTOMER** Confidential Information is encrypted both in transit and at rest using industry-accepted encryption standards.
- Prohibit the storage or transportation of **CUSTOMER** Confidential Information on removable media unless expressly approved in writing by the **CUSTOMER**.
- Ensure all external network communications utilize Transport Layer Security (TLS) version 1.2 or higher (or successor standard approved by **CUSTOMER**).
- Store **CUSTOMER** data exclusively within the geographical boundaries of the United States unless otherwise approved in writing by **CUSTOMER**.
- Comply with **CUSTOMER**'s Prohibited Technologies Policy and any successor policies adopted during the Contract term.

- Obtain prior written approval from **CUSTOMER** before permitting personnel located outside the United States to access **CUSTOMER** systems or **CUSTOMER** data.

CUSTOMER may request additional administrative or security documentation throughout the Contract term to support audits, regulatory requirements, risk management activities, or other legitimate business needs.

Nothing in this section relieves **VENDOR** of its responsibility to comply with the operational Security and Compliance requirements established in the RFO.

6. Contract Administration

The Contract Administration requirements established in this section are intended to support effective administration of the Contract and shall complement, but not replace, the governance, delivery management, engineering, and operational responsibilities established throughout the RFO. Nothing in this section shall be interpreted as transferring responsibility for delivery outcomes or operational performance from **VENDOR** to **CUSTOMER**.

6.1 Deliverable Review and Acceptance

CUSTOMER shall review all Deliverables expressly listed in Section 4.9 herein submitted by **VENDOR** to determine whether they satisfy the requirements established under this Contract and the RFO. Deliverables shall be complete, accurate, and submitted in accordance with the applicable requirements, schedules, and acceptance criteria established throughout this Contract.

Unless otherwise specified, **VENDOR** shall notify **CUSTOMER** when a deliverable is ready for review. **CUSTOMER** shall review the deliverable within a reasonable period and may:

- Accept the deliverable;
- Reject the deliverable and identify deficiencies requiring correction; or
- Request clarification or additional information necessary to complete the review.

If **CUSTOMER** identifies deficiencies, **VENDOR** shall correct the identified deficiencies at no cost to **CUSTOMER** and resubmit the deliverable for review within a mutually agreed upon timeframe. The review and resubmission process shall continue until the deliverable satisfies the applicable Contract requirements.

Acceptance of a deliverable signifies that the deliverable satisfies the applicable requirements identified during **CUSTOMER**'s review. Acceptance

shall not relieve **VENDOR** of responsibility for latent defects, omissions, errors, security vulnerabilities, noncompliance with the Contract, or other deficiencies subsequently identified during the Contract term.

Recurring operational deliverables, including reports, dashboards, governance artifacts, and other routine deliverables, shall be reviewed through the governance processes established under the RFO unless otherwise specified by **CUSTOMER**.

CUSTOMER's review or acceptance of any deliverable shall not transfer responsibility for the quality, completeness, accuracy, security, maintainability, operational performance, or successful delivery of the Managed Services. **VENDOR** remains fully responsible for satisfying all requirements of this Contract.

6.2 Contract Change Management

CUSTOMER recognizes that business priorities, technologies, funding, legislative requirements, and operational needs may evolve throughout the Contract term. Changes affecting the scope, pricing, schedule, deliverables, or other contractual requirements of this Contract shall be managed through a formal Contract Change Management process.

The Contract Change Management process established in this section shall serve as the exclusive mechanism for modifying the scope of services, Contract pricing, deliverables, schedule, or other contractual obligations. No verbal approvals, informal communications, or other undocumented agreements shall modify the requirements of this Contract.

VENDOR shall promptly notify **CUSTOMER** of any circumstance that may require a modification to the Contract, including changes that may materially affect the scope of services, Contract pricing, staffing, schedule, deliverables, assumptions, dependencies, or other contractual obligations.

Either party may request a Contract modification by submitting a written Change Request describing the proposed change, the business or technical justification, the anticipated impacts, and any recommended alternatives.

At a minimum, each Change Request shall include:

- A detailed description of the proposed change.
- The business or technical justification for the change.
- A comprehensive impact assessment, including impacts to scope, cost, schedule, technical architecture, operational performance, security, quality, and other contractual obligations, as applicable.
- Identification of assumptions, dependencies, risks, and constraints.

- Alternatives considered, where applicable.
- The requested implementation timeline, where applicable.
- Proposed pricing adjustments and supporting cost justification, where applicable.

VENDOR shall cooperate with **CUSTOMER** in evaluating proposed Contract changes and shall provide sufficient information to support informed decision-making.

No Contract modification shall become effective unless approved in writing by authorized representatives of both parties in accordance with applicable State of Texas procurement requirements and the terms of the Contract.

Nothing in this section limits **CUSTOMER's** ability to reprioritize work, modify the Product Backlog, adjust Sprint priorities, or redirect work within the scope of the Managed Services engagement through the governance processes established under the RFO, provided such changes do not materially alter the scope of the Contract.

6.3 Contract Administration

CUSTOMER intends to establish a long-term Managed Services partnership that promotes operational stability, continuous improvement, and successful delivery of the services described in this RFO. **CUSTOMER** and **VENDOR** shall maintain open communication and collaborate to support effective contract administration, timely resolution of contractual and administrative matters, and successful delivery of the Managed Services throughout the Contract term.

CUSTOMER shall designate a Contract Manager who shall serve as the primary point of contact for contract administration, coordination, and oversight. **VENDOR** shall designate an Engagement Manager or other authorized representative who shall serve as **VENDOR's** primary point of contact for contract administration and shall coordinate with the appropriate members of **VENDOR's** Delivery Organization regarding operational, technical, and administrative matters.

CUSTOMER's Contract Manager and **VENDOR's** designated representative shall work collaboratively throughout the Contract term to:

- Coordinate day-to-day contract administration activities.
- Monitor compliance with the Contract and RFO.
- Review required reports, deliverables, and other Contract documentation.
- Coordinate Contract modifications and administrative actions, as necessary.

- Facilitate communication between **CUSTOMER**, **VENDOR**, and other stakeholders.
- Coordinate audits, records requests, and other administrative activities related to the Contract.
- Resolve contractual or administrative issues in a timely manner.

Operational management of the Managed Services engagement shall occur through the governance framework established in Section 4.6 of this RFO and shall not replace or diminish the responsibilities of the designated Contract Manager.

6.4 Vendor Accountability

VENDOR is solely responsible for the performance of all contractual obligations under this Agreement. The use of subcontractors or third-party providers does not relieve **VENDOR** of any responsibility or liability for the performance, quality, timeliness, security, or compliance of the Services.

If **VENDOR** fails to meet the required service levels, deliverables, or contractual requirements, **CUSTOMER** reserves the right to obtain the required services from another source and recover any reasonable additional costs incurred, including the costs associated with procuring replacement services.

7. Pricing and Payment Term

7.1 Pricing Structure

RESPONDENT shall propose a fixed-fee pricing model that supports the successful delivery of the Managed Services described in the RFO. Proposed pricing shall be all-inclusive and include all labor, management, supervision, software engineering, solution architecture, quality engineering, DevSecOps, cloud operations, production support, governance, documentation, project management, software licensing, tools, maintenance, overhead, travel, administrative support, and all other costs necessary to perform the services required under this Contract, unless otherwise expressly identified by **CUSTOMER**.

CUSTOMER intends to procure dedicated Managed Services delivery capacity through recurring Sprint Cycles rather than individual technical resources, labor categories, or hourly services. The proposed pricing shall reflect **VENDOR's** responsibility to organize, staff, manage, and continuously improve the Delivery Organization necessary to successfully perform all services described in the RFO.

CUSTOMER anticipates a delivery model consisting of two dedicated cross-functional Agile delivery teams:

- **Design, Development, and Implementation (DDI) Delivery Team**

Responsible for application design, software engineering, application enhancements, modernization initiatives, solution architecture, quality engineering, DevSecOps, release management, and the delivery of new business capabilities.

- **Support and Maintenance Services (SMS) Delivery Team**

Responsible for production operations, application maintenance, production support, incident and problem management, operational stability, security remediation, compliance activities, documentation, and the ongoing sustainment of the managed application portfolio.

The DDI Delivery Team and SMS Delivery Team shall collectively support **CUSTOMER**'s entire College and Career Advising technology portfolio and provide the delivery capacity necessary to perform all services described in the RFO throughout the Contract term. Each proposed delivery team shall provide sufficient dedicated capacity to perform all responsibilities assigned to that team throughout each Sprint Cycle. Pricing shall be based upon the fixed delivery capacity provided by each delivery team during each Sprint Cycle and shall not be based upon hours worked, individual labor categories, or the number of personnel assigned to the engagement.

CUSTOMER recognizes that the composition, staffing model, and skill mix of each delivery team may vary based upon **RESPONDENT**'s proposed delivery methodology and organizational approach. Accordingly, **RESPONDENT** shall propose the organizational structure it believes is necessary to successfully perform the required services.

VENDOR shall remain fully responsible for ensuring that each delivery team possesses the collective technical expertise, capacity, leadership, and engineering disciplines necessary to satisfy all Contract requirements. **VENDOR** shall remain solely responsible for staffing, workload balancing, resource allocation, succession planning, cross-training, and personnel continuity necessary to successfully perform the services required under this Contract.

7.2 Pricing Schedule

At a minimum, **RESPONDENT** shall submit a Pricing Schedule using the following format, or an equivalent format that includes the same information.

Delivery Team	Fixed Price per Sprint Cycle	Sprint Cycles per Contract Year	Annual Fixed Price
Design, Development, and Implementation Delivery Team	\$		\$
Support and Maintenance Services Delivery Team	\$		\$
Total Annual Contract Price			\$

The proposed fixed price per Sprint Cycle shall remain in effect throughout the initial Contract term and any renewal periods exercised by **CUSTOMER** unless otherwise modified through a written Contract amendment executed by both parties.

RESPONDENT shall identify any assumptions that materially affect its proposed pricing, including assumptions regarding Sprint Cycle duration, **CUSTOMER** participation, application portfolio scope, environments, third-party services, or other factors that materially influence its proposed pricing.

Changes that materially increase or decrease the scope of the Managed Services beyond the requirements established in the RFO may be addressed through the Contract Change Management process established under this Contract.

7.3 Invoicing and Payment

VENDOR shall submit invoices in accordance with the terms of the Contract and **CUSTOMER's** invoicing requirements. Invoices shall be submitted following completion of the applicable Sprint Cycle(s) or other billing period established under the Contract and following **CUSTOMER** acceptance of the corresponding Managed Services performed during that billing period.

Invoices shall accurately reflect the Sprint Cycles performed and the corresponding Managed Services delivered during the applicable billing period. **VENDOR** shall provide reasonable supporting documentation necessary to enable **CUSTOMER** to verify the services invoiced, including governance reports, Sprint summaries, performance reports, or other documentation demonstrating that the Managed Services were delivered in

accordance with the Contract. **CUSTOMER** reserves the right to request additional documentation reasonably necessary to verify invoice accuracy or demonstrate compliance with the Contract.

Invoices shall be submitted electronically to **CUSTOMER**'s Accounts Payable office at accountspayable@highered.texas.gov and to the designated **CUSTOMER** Contract Manager(s), unless otherwise directed by **CUSTOMER**. At a minimum, each invoice shall include:

- **VENDOR** name, mailing address, email address, and telephone number.
- Name, email address, and telephone number of **VENDOR** representative responsible for invoice inquiries.
- **CUSTOMER** name, Agency Number (781), and Address.
- Purchase Order and/or Contract Number.
- Invoice Number and Invoice Date.
- Billing Period.
- Texas Identification Number (TIN) issued by the Texas Comptroller.
- Identification of the applicable Sprint Cycles invoiced for the Design, Development, and Implementation Delivery Team and the Support and Maintenance Services Delivery Team.
- Fixed Price per Sprint Cycle.
- Total Amount Due for the billing period.
- If applicable, the Texas Identification Number (TIN) of both the original contractor and any authorized successor contractor following an approved assignment of the Contract.
- Any other information reasonably required by **CUSTOMER** to support invoice review and payment.

CUSTOMER shall review Invoices for accuracy and compliance with the Contract. **CUSTOMER** may dispute any invoice, or portion thereof, that is inaccurate, unsupported, inconsistent with the Contract, or includes charges not authorized under the Contract. **CUSTOMER** shall notify **VENDOR** of any disputed amounts and the basis for the dispute. **VENDOR** shall cooperate with **CUSTOMER** to promptly resolve any invoice discrepancies.

Payment shall be made only after **CUSTOMER** has verified that the invoiced Managed Services have been satisfactorily performed and accepted in accordance with the requirements of the Contract and RFO.

CUSTOMER shall make payment of undisputed invoice amounts in accordance with the Texas Prompt Payment Act (Tex. Gov't Code, Chapter 2251) and other applicable State of Texas requirements.

Payment by **CUSTOMER** shall not constitute acceptance of deficient services, waive any rights or remedies available under the Contract, or relieve **VENDOR** of responsibility for satisfying all requirements of the Contract and the RFO. **CUSTOMER** will not pay for any services provided prior to Contract execution. The Contract is subject to appropriations and the continuing availability of funds.

8. Solicitation Key Deadlines and Events

8.1 Procurement Schedule

RESPONDENTS should review the Calendar of Events table below for a schedule of events and deadlines for this procurement.

Calendar of Events

Event	Anticipated Date
Publication of RFO	October 1, 2026
Deadline for Written Questions	October 9, 2026 – 11:30 PM CT
Anticipated Responses to Written Questions	October 16, 2026
Proposal Due Date and Time	October 22, 2026 – 11:30 PM CT
Oral Presentations (If Required)	TBD
Anticipated Contract Award	TBD
Anticipated Contract Start Date	January 1, 2027

CUSTOMER reserves the right to revise the procurement schedule, extend deadlines, or modify any aspect of this RFO by issuing an Addendum through [THECB's Vendor Client Gateway](#).

RESPONDENTS are responsible for monitoring [THECB's Vendor Client Gateway](#) throughout the RFO period and for ensuring they are aware of all Addenda and other procurement communications issued by **CUSTOMER**.

8.2 Proposal Due Date

RESPONDENTS shall submit their Proposals no later than the Proposal Due Date and time identified in the Calendar of Events above. Proposals received after the stated deadline will be rejected as late and will not be considered for evaluation.

RESPONDENTS may be required to provide proof of timely submission upon request. **CUSTOMER** shall not be responsible for Proposals that are delayed, rejected, blocked, filtered, quarantined, corrupted, or otherwise prevented

from reaching the designated submission location due to internet connectivity issues, email transmission failures, security software, system outages, or other circumstances beyond **CUSTOMER's** control.

8.3 Procurement Point of Contact

RESPONDENTS shall direct all inquiries, written questions, requests for clarification, and other communications concerning this RFO exclusively to the Procurement Point of Contact identified below through [THECB's Vendor Client Gateway](#), except as otherwise expressly authorized by **CUSTOMER**.

Miriam Hogans, CTCD, CTCM

Miriam.Hogans@highered.texas.gov

Contract Developer

Financial Services Division

Texas Higher Education Coordinating Board

All communications shall reference **RFO No. 781-6-CB-20**

Except as expressly authorized by the Procurement Point of Contact, **RESPONDENTS** shall not contact or attempt to contact other **CUSTOMER** employees, including Commissioners, executive leadership, evaluation committee members, program staff, or their representatives, regarding this RFO. Unauthorized communications may result in **RESPONDENT's** Proposal being determined non-responsive or otherwise disqualified from further consideration.

Only written responses issued by **CUSTOMER** shall be considered official and binding. Any clarification, interpretation, modification, or other information determined by **CUSTOMER** to be of general interest or that affects the requirements of this RFO shall be communicated through an Addendum or other written notice published on the [THECB's Vendor Client Gateway](#).

Written questions related to VetHUB Subcontracting Plans may be directed to: HUB@highered.texas.gov.

The Procurement Point of Contact may designate an alternate representative or authorize another **CUSTOMER** representative to communicate with **RESPONDENTS** for limited purposes, including procurement administration, contract negotiations, or other activities related to this RFO.

8.4 Questions and Answers

CUSTOMER will accept written questions or requests for clarification regarding this RFO through [THECB's Vendor Client Gateway](#) to provide **RESPONDENTS** with a better understanding of **CUSTOMER's** requirements and expectations prior to submitting their Proposals.

To ensure a fair, transparent, and competitive procurement process, all clarification questions shall be submitted no later than the deadline identified in the Calendar of Events. Questions received after the published deadline will not be answered.

CUSTOMER's responses to submitted questions will be posted on [THECB's Vendor Client Gateway](#). Questions and responses will be shared with all prospective **RESPONDENTS** through [THECB's Vendor Client Gateway](#). The identity of the **RESPONDENT** submitting a question will not be disclosed.

RESPONDENTS shall promptly notify the Procurement Point of Contact of any ambiguity, conflict, discrepancy, omission, restrictive specification, or other error identified in this RFO prior to the deadline for submitting written questions. Failure to timely notify **CUSTOMER** of such conditions shall constitute a waiver of any claim arising from ambiguity, conflict, discrepancy, omission, restrictive specification, or other alleged error in this RFO or any resulting Contract.

RESPONDENTS are responsible for monitoring the Electronic State Business Daily and [THECB's Vendor Client Gateway](#) throughout the solicitation period for procurement communications issued by **CUSTOMER**.

8.5 Proposal Submission

RESPONDENT's submission of a Proposal constitutes a binding offer to contract based on the terms, conditions, and specifications set forth in this RFO. By submitting a Proposal, **RESPONDENT** represents and warrants that the Proposal has been executed by an individual authorized to legally bind **RESPONDENT** and that **RESPONDENT** has the authority, capability, and intent to perform the Services if selected for Contract award.

8.6 Proposal Modification and Withdrawal

RESPONDENT may withdraw or modify its Proposal at any time prior to the Proposal submission deadline by submitting written notice through [THECB's Vendor Client Gateway](#). Once the submission deadline has passed, **RESPONDENT** may not withdraw or modify a Proposal except as expressly permitted by applicable State of Texas law or by the **CUSTOMER** through the procurement process.

If **RESPONDENT** requests to modify a Proposal, **RESPONDENT** shall clearly identify the portion(s) of the Proposal being amended or replaced and shall include any revised documents necessary to fully implement the requested modification. All requests to withdraw or modify a Proposal shall be signed by an individual authorized to legally bind **RESPONDENT**.

9. Proposal Submission Requirements

RESPONDENT shall submit a complete and responsive Proposal that addresses all requirements of this RFO and complies with the submission instructions, format, content, and deadlines established herein. **RESPONDENT** is solely responsible for ensuring that its Proposal is complete, accurate, well organized, internally consistent, and fully responsive to the requirements of this RFO.

Mailed, hand-delivered, facsimile, or other unauthorized submissions will not be accepted.

RESPONDENT should limit the use of embedded hyperlinks within a Proposal as **CUSTOMER** cannot guarantee that evaluators will have access to external websites, cloud repositories, or other linked resources during the evaluation process. **RESPONDENT** should include all information necessary for the evaluation of the Proposal directly within the Proposal whenever practicable.

Failure to comply with the requirements of this RFO may result in the Proposal being determined non-responsive or otherwise ineligible for further consideration.

Proposals shall adhere to the following submission requirements:

- Be submitted **electronically** through the [THECB Vendor Client Gateway](#) by the Proposal submission deadline noted in Section 8.
- Be submitted by an individual authorized to legally bind **RESPONDENT**.

Proposals must include the following two files, as described in more detail below:

- 1) **Pricing Proposal** (See Section 9.6 and Section 7)
 - 2) **Solution Proposal**, in a single searchable PDF format, that includes the following:
 - Section 9.1 – Executive Summary
 - Section 9.2 – Company References
 - Section 9.3 – Company Experience
 - Section 9.4 – Delivery Organization and Key Personnel
 - Section 9.5 – Technical Proposal
 - Section 9.7 – Exceptions, Assumptions, and Risks
 - Section 9.8 – Required Forms, Certifications, & Disclosures
- Provide sufficient detail to enable **CUSTOMER** to evaluate **RESPONDENT's** organizational qualifications, technical capabilities, delivery methodology, staffing approach, pricing, and overall ability to successfully perform the Managed Services described in the RFO.

- Clearly demonstrate **RESPONDENT's** understanding of **CUSTOMER's** business objectives, technical environment, service delivery expectations, and contractual requirements.

9.1 Executive Summary

RESPONDENT shall provide an Executive Summary that presents a concise overview of **RESPONDENT's** Proposal, including its overall understanding of **CUSTOMER's** objectives and approach to providing the Managed Services described in this RFO.

The Executive Summary must be signed by an individual authorized to legally bind the **RESPONDENT** and must confirm that the Proposal shall remain valid for a minimum of one hundred twenty (120) calendar days following the Proposal submission deadline.

The Executive Summary shall include:

- **RESPONDENT's** understanding of **CUSTOMER's** objectives and business needs.
- A high-level summary of **RESPONDENT's** proposed Managed Services solution.
- An overview of the proposed delivery organization and service delivery approach.
- A summary of **RESPONDENT's** qualifications and experience relevant to the engagement.
- Key differentiators and value **RESPONDENT** proposes to deliver to **CUSTOMER**.

9.2 Company References

RESPONDENT shall provide a minimum of three (3) client references for engagements of similar scope, size, and complexity successfully performed within the past five (5) years. To the extent practicable, the references should represent organizations with comparable operational, technical, regulatory, or governance requirements, including public sector organizations, institutions of higher education, or other organizations of similar complexity.

For each reference, **RESPONDENT** shall provide:

- Client organization;
- Project or engagement description;
- Services provided;
- Contract term;

- Client point of contact, including name, title, email address, and telephone number, if possible; and
- A brief description of the outcomes achieved and **RESPONDENT's** role in the engagement.

CUSTOMER reserves the right to contact any reference provided by **RESPONDENT** to verify the information contained in the Proposal. In addition, **CUSTOMER** may consider information obtained from other available and credible sources, including current or former customers, publicly available information, performance evaluations, and **CUSTOMER's** own experience with **RESPONDENT**, when evaluating **RESPONDENT's** qualifications, past performance, and demonstrated ability to successfully perform the Services described in this RFO.

9.3 Company Experience

RESPONDENT shall demonstrate organizational experience delivering enterprise application development, application maintenance, production support, Agile software delivery, DevSecOps, cloud operations, quality engineering, and related technology services for organizations of similar size and complexity. Experience supporting public sector organizations, cloud-based application platforms, enterprise integrations, customer-facing digital services, and modern software engineering practices is preferred.

The Proposal shall provide sufficient information for **CUSTOMER** to evaluate **RESPONDENT's** organizational maturity, relevant experience, technical capabilities, and ability to successfully support **CUSTOMER's** College and Career Advising technology portfolio.

RESPONDENT shall provide:

- A **brief history and overview of the organization**, including the year established, corporate headquarters, ownership structure, and primary lines of business.
- The **size of the organization**, including the approximate number of employees and the **locations** from which services supporting this engagement will be provided.
- A **description of RESPONDENT's experience** providing Managed Services of **similar scope, size, and complexity**, particularly for cloud-hosted, Agile software development and application support engagements.
- A **description of RESPONDENT's experience** delivering **secure** Managed Services, including secure software development practices,

cloud security, production support, incident response, accessibility compliance, and operational monitoring capabilities.

- A **description of RESPONDENT's experience supporting public sector organizations**, institutions of higher education, or other organizations with comparable governance, regulatory, cybersecurity, and operational requirements.
- A **summary of RESPONDENT's experience with technologies, platforms, and engineering disciplines relevant** to this engagement, including, as applicable, Microsoft Azure, Azure DevOps, Microsoft Entra ID, Azure SQL, .NET, JavaScript frameworks, API development, DevSecOps, Quality Engineering, cloud operations, and cybersecurity.
- **Documentation describing projects or engagements of similar scope, complexity, and scale** performed within the past five (5) years, including project descriptions, technologies utilized, services provided, and outcomes achieved.
- A summary of any relevant industry certifications, professional accreditations, strategic partnerships, or organizational qualifications that demonstrate **RESPONDENT's** ability to successfully perform the services described in this RFO.

9.4 Delivery Organization and Key Personnel

9.4.1 Delivery Organization

RESPONDENT shall provide a narrative of **RESPONDENT's** organizational approach to delivering Managed Services, including organizational structure, staffing strategy, governance, service delivery, continuous improvement, knowledge management, and operational excellence.

At a minimum, **RESPONDENT** shall include the following:

- A **description of RESPONDENT's Delivery Organization Model and delivery methodology**, including its approach to Agile project management, engineering governance, architecture review, DevSecOps, release management, quality assurance, continuous improvement, and operational support.
- An **organizational chart** illustrating the proposed Delivery Organization and reporting relationships for personnel supporting the engagement.

- A **description of the proposed organizational structure**, including the Design, Development, and Implementation Delivery Team and the Support and Maintenance Services Delivery Team.
- A **description of the responsibilities assigned** to each team and how the proposed organization will support application operations, software engineering, cloud operations, quality engineering, DevSecOps, cybersecurity, governance, and continuous improvement.
- A **description of the staffing strategy, resource management approach, succession planning, cross-training practices, and knowledge management processes** that will be used to maintain continuity of service throughout the Contract term.
- A **description of the proposed staffing model**, including the use of on-site and remote personnel. The **RESPONDENT** shall identify the primary work location of personnel assigned to the engagement.
- A **description of RESPONDENT's software engineering quality practices**, including peer code reviews, automated testing, regression testing, accessibility validation, application security testing, vulnerability scanning, and release quality assurance processes.

9.4.2 Key Personnel

RESPONDENT shall identify the key leadership personnel who will be responsible for managing and overseeing the engagement, including, at a minimum:

- Engagement Manager (or Account Manager)
- Product Manager
- Delivery Manager(s) / Project Manager
- Scrum Master
- Technical Architect
- Engineering Lead
- UI/UX Lead
- Content Lead
- Quality Engineering Lead
- Quality Assurance Lead

For each identified individual, the **RESPONDENT** shall provide:

- Name and Proposed Role;
- Resume or other summary of relevant qualifications and experience;
- Applicable professional certifications;
- Years of experience supporting similar engagements; and
- Employment status as contractor or employee with **RESPONDENT**.

CUSTOMER recognizes that staffing may evolve throughout the Contract term and does not require resumes for all personnel proposed to support the engagement. However, resumes shall be provided for all identified Key Personnel and shall clearly demonstrate the qualifications and experience necessary to successfully perform their assigned responsibilities.

If **RESPONDENT** intends to utilize subcontractors, the Proposal shall clearly identify each subcontractor, describe the services to be provided, and identify the roles and responsibilities assigned to subcontractor personnel.

VENDOR shall remain fully responsible for the performance of all personnel and subcontractors assigned to the engagement, regardless of employment or contractual relationship.

9.5 Technical Proposal

RESPONDENT shall submit a Technical Proposal describing its approach to successfully delivering the Managed Services described in this RFO. The Technical Proposal shall demonstrate **RESPONDENT**'s understanding of **CUSTOMER**'s objectives, proposed delivery methodology, organizational capability, engineering practices, governance approach, and overall ability to successfully perform the services required under this RFO and any resulting Contract.

The Technical Proposal shall clearly describe how **RESPONDENT** intends to organize, manage, and continuously improve the Managed Services throughout the Contract term.

At a minimum, the Technical Proposal shall address the following:

9.5.1 Delivery Organization

Describe the proposed Delivery Organization, including the organizational structure, management approach, reporting

relationships, and overall service delivery model that will be used to support **CUSTOMER** throughout the Contract term.

9.5.2 Service Delivery Approach

Describe the overall approach to delivering the Managed Services, including application operations, maintenance, software engineering, modernization, cloud operations, quality engineering, DevSecOps, cybersecurity, documentation, governance, and continuous improvement.

9.5.3 Agile Delivery Methodology

Describe the proposed Agile delivery methodology, including sprint planning, backlog management, estimation, release planning, quality management, stakeholder engagement, and continuous improvement practices.

9.5.4 Technical and Engineering Approach

Describe the engineering practices, technical standards, architecture approach, quality engineering practices, DevSecOps methodology, cloud operations, cybersecurity practices, documentation standards, and operational support model that will be used to deliver the services described in the RFO.

9.5.5 Governance and Performance Management

Describe the proposed governance framework, communication approach, performance management methodology, reporting practices, risk management processes, issue escalation procedures, and continuous improvement program.

9.5.6 Service Transition

Describe the approach for assuming responsibility for the Managed Services, including knowledge transfer, operational readiness, onboarding, discovery, documentation validation, transition planning, and transition to steady-state operations.

9.5.7 Innovation and Continuous Improvement

Describe how **RESPONDENT** will proactively identify opportunities to improve application architecture, software quality, cybersecurity, cloud operations, operational efficiency, engineering maturity, customer experience, and overall service delivery throughout the Contract term.

CUSTOMER encourages **RESPONDENT**s to leverage the experience, methodologies, engineering practices, tools, and organizational capabilities

they believe best support the successful delivery of the Managed Services described in this RFO. The Technical Proposal should demonstrate how **RESPONDENT**'s proposed approach aligns with the requirements established in the RFO while delivering value through innovation, operational excellence, continuous improvement, and a collaborative partnership focused on the long-term success and evolution of **CUSTOMER**'s technology portfolio.

9.6 Pricing Proposal

RESPONDENT shall submit a separate Pricing Proposal in accordance with all requirements established in Section 7 of this RFO.

The Pricing Proposal shall be completed using the Pricing Workbook provided as part of this RFO or another format proposed by **RESPONDENT** that clearly presents the same information and level of detail. The Pricing Proposal shall be complete, accurate, and include all pricing necessary to perform the Managed Services described in the RFO.

CUSTOMER reserves the right to request clarification of pricing information during the evaluation process. Such requests shall not permit **RESPONDENT** to modify its proposed pricing except as expressly authorized by **CUSTOMER** through the procurement process.

Pricing shall remain valid for a minimum of one hundred twenty (120) calendar days following the Proposal submission deadline unless otherwise extended by mutual written agreement.

9.7 Exceptions, Assumptions, and Risks

RESPONDENT must identify any requested exceptions to this RFO or the anticipated Contract in its Proposal. **RESPONDENT** shall clearly identify all Exceptions by Section and include a proposed alternative. Failure to identify requested exceptions shall constitute the **RESPONDENT**'s acceptance of the RFO requirements as issued.

RESPONDENT cannot take a "blanket exception" to the entire RFO. If any **RESPONDENT** takes a "blanket exception" to this entire RFO or does not provide proposed alternative language, the proposal may be disqualified from further consideration. Please note as an agency of the state of Texas, **CUSTOMER** is bound to comply with all applicable state and federal procurement and contract laws.

RESPONDENT shall further identify any assumptions, dependencies, prerequisites, exclusions, or risks that materially affect its proposed solution, staffing approach, pricing, implementation schedule, or ability to successfully perform the Services described in this RFO. Failure to identify assumptions or dependencies shall constitute the **RESPONDENT**'s representation that it can

perform the Services in accordance with the requirements of this RFO and any resulting Contract.

9.8 Required Forms, Certifications, and Disclosures

9.8.1 Attachment A - Respondent Info

RESPONDENT shall complete and return all forms contained within Attachment A. Failure to complete these forms may render **RESPONDENT's** Proposal non-responsive.

9.8.2 Conflict of Interest Disclosure Statement

RESPONDENTS shall be neutral and impartial and shall not advocate specific positions to THECB. Entities having a conflict of interest, as determined solely by THECB, will not be eligible for a contract award.

Respondent's submitted Conflict of Interest Disclosure Statement must meet the following requirements:

- Be attested to by an unsworn declaration;
- Identify either the extent, nature, and length of any potential relationships or engagements that require disclosure or a statement that no known or potential conflicts of interest exist;
- Address how Respondent intends to ensure that no interest arises or potentially arises because of its activities or those of its parent, affiliate, or other related entity that would conflict with Respondent's duty should it be selected to provide these services; and
- Be signed by the highest-ranking officer of Respondent's entity having responsibility for vetting corporate conflicts of interest, e.g., a corporate Executive Vice President rather than the head of an operating or regional unit of the firm.

Failure to provide either a signed statement on potential conflicts of interest or a signed statement that no potential conflicts exist may disqualify RESPONDENT.

THECB may not enter into a contract with a person it has employed within the past twelve (12) months. Individuals who have been employed by THECB or by another state agency in Texas more than twelve (12) months but fewer than twenty-four (24) months ago shall disclose in the proposal the nature of previous employment with the state agency and the date the employment ended.

10. Proposal Evaluation

CUSTOMER will evaluate responsive Proposals to this RFO based on the evaluation criteria noted below to determine which **RESPONDENT** offers the best value to the State of Texas. This procurement is intended to establish a long-term Managed Services partnership rather than procure individual technical resources or staff augmentation services. Accordingly, the evaluation will emphasize **RESPONDENT's** ability to deliver a mature, outcome-oriented service model through effective governance, Agile delivery, engineering excellence, operational maturity, continuous improvement, and customer partnership.

10.1 Evaluation Criteria

CUSTOMER will evaluate Proposals using the criteria described below. The relative weight of each criterion is indicated in the left-hand column. **CUSTOMER** may consider both the final weighted score as well as the average ranking when making vendor selection(s).

Weight	Evaluation Criteria
35%	Technical Proposal and Managed Services Approach
20%	Organizational Qualifications and Experience
10%	Delivery Organization and Key Personnel
25%	Pricing Proposal
10%	Responsiveness, Clarity, and Organization of the Proposal
100%	Total

10.1.1 Technical Proposal and Managed Services Approach

CUSTOMER will evaluate **RESPONDENT's** understanding of the engagement and its proposed approach to delivering the Managed Services described in the RFO.

Evaluation may include, but is not limited to:

- Understanding of **CUSTOMER's** objectives, business needs, and technology environment.
- Proposed Managed Services delivery model.
- Delivery Organization, governance approach, and service management methodology.
- Agile delivery practices and software engineering methodology.
- Architecture, Quality Engineering, DevSecOps, cloud operations, cybersecurity, and operational support capabilities.
- Continuous improvement methodology.
- Service Transition approach.

- Overall technical quality and completeness of the proposed solution.

10.1.2 Organizational Qualifications, Experience, and Past Performance

CUSTOMER will evaluate **RESPONDENT**'s demonstrated experience providing Managed Services for organizations of similar size, complexity, and operational requirements.

Evaluation may include:

- Experience providing enterprise Managed Services.
- Experience supporting cloud-hosted application portfolios.
- Experience supporting Agile software delivery.
- Experience supporting public sector organizations, institutions of higher education, or organizations with comparable governance and regulatory requirements.
- Organizational maturity.
- Past performance on comparable engagements.
- Client references.

10.1.3 Delivery Organization and Key Personnel

CUSTOMER will evaluate the proposed Delivery Organization and the qualifications of the key leadership personnel responsible for managing the engagement.

Evaluation may include:

- Organizational structure.
- Leadership and management approach.
- Relevant experience and professional certifications for key personnel.
- Staffing strategy.
- Knowledge management and succession planning.
- Ability to provide sufficient delivery capacity throughout the Contract term.
- Overall capability of the proposed Delivery Organization.

10.1.4 Pricing Proposal

CUSTOMER will evaluate the Pricing Proposal to determine its reasonableness, completeness, competitiveness, and overall value.

CUSTOMER will evaluate pricing in the context of **RESPONDENT's** proposed Managed Services solution and overall ability to successfully deliver the services described in the RFO. **CUSTOMER** is not obligated to award a Contract to **RESPONDENT** submitting the lowest-priced Proposal.

10.1.5 Responsiveness, Clarity, and Organization of the Proposal

The **CUSTOMER** will evaluate each Proposal for responsiveness to the requirements of this RFO.

Evaluation may include:

- Compliance with RFO requirements.
- Organization and clarity.
- Completeness.
- Professional presentation.
- Responsiveness to the RFO.
- Overall quality of the Proposal.

10.2 Proposal Scoring Methodology

Each evaluation criterion will be scored independently by the evaluation committee using the following rating scale. Scores will be multiplied by the applicable weighting assigned to each evaluation criterion to determine the **RESPONDENT's** weighted evaluation score.

Score	Rating	Description
5	Exceptional	Proposal significantly exceeds the requirements of the RFO. The response demonstrates exceptional understanding, capability, and value with minimal or no identified weaknesses.
4	Good	Proposal exceeds the requirements in several meaningful areas and demonstrates a strong understanding of the CUSTOMER's needs with only minor weaknesses.
3	Acceptable	Proposal satisfactorily meets the requirements of the RFO and demonstrates an acceptable approach with no significant deficiencies.
2	Marginal	Proposal addresses many of the requirements but contains weaknesses, omissions, or risks that

Score	Rating	Description
		reduce confidence in the RESPONDENT 's ability to successfully perform the Services.
1	Poor	Proposal minimally addresses the requirements and contains significant weaknesses, deficiencies, or risks that substantially reduce confidence in successful performance.
0	Unacceptable	Proposal fails to address the evaluation criterion or demonstrates that the RESPONDENT cannot satisfy the requirements of the RFO.

10.3 Scoring and Evaluation Process

10.3.1 Administrative Review

CUSTOMER will conduct an administrative review of all Proposals to verify compliance with the mandatory submission requirements of this RFO, including the submission of all required Proposal components, pricing information, forms, certifications, disclosures, and supporting documentation. **CUSTOMER** reserves the right to determine whether a Proposal is complete and responsive. Failure to submit required information or supporting documentation may result in the Proposal being determined non-responsive or otherwise ineligible for further consideration.

10.3.2 Evaluation

CUSTOMER will evaluate Proposals that meet all submission requirements and satisfy the minimum qualifications. **CUSTOMER** will evaluate responsive Proposals using the weighted evaluation criteria identified above. **CUSTOMER** may conduct one or more additional evaluation activities, including written clarifications, oral presentations, demonstrations, reference checks, interviews, or other due diligence activities, as determined necessary.

10.3.3 Clarifications, Oral Presentations, and Interviews

CUSTOMER reserves the right to request written clarifications, supplemental information, or administrative corrections from one or more **RESPONDENTS** during the evaluation process. Such requests shall not permit **RESPONDENT** to revise its Technical Proposal, Pricing Proposal, or any other material aspect of its Proposal unless expressly authorized by **CUSTOMER** as part of the procurement process.

At the sole discretion of **CUSTOMER**, one or more **RESPONDENTS** may be invited to participate in an Oral Presentation or Interview as part of the Proposal evaluation process to provide **CUSTOMER** with an opportunity to better understand **RESPONDENT**'s proposed Managed Services approach or interview Key Personnel.

CUSTOMER may request participation by specific members of the proposed Delivery Organization, including the Engagement Manager, Delivery Manager(s), Technical Architect, Engineering Lead, Quality Engineering Lead, Product Owner(s), or other Key Personnel identified in the Proposal. **CUSTOMER** encourages participation by the personnel expected to have primary responsibility for managing and delivering the Managed Services throughout the Contract term.

Following completion of the Oral Presentations, the evaluation committee may revise evaluation scores, if warranted, based on the information, clarifications, and responses provided during the Oral Presentation or Interview. Evaluation scores may increase or decrease because of the Oral Presentation. The revised evaluation score shall be considered the final evaluation score for purposes of determining the Proposal representing the best value to the State of Texas.

Failure of a **RESPONDENT** to participate in a requested Oral Presentation or Interview may result in the Proposal being removed from further consideration. **CUSTOMER** is not responsible for any costs incurred by the **RESPONDENT** in preparation for, attendance at, participation in, or otherwise related to any Oral Presentation or Interview. All such costs shall be the sole responsibility of the **RESPONDENT**.

10.3.4 Contract Award

CUSTOMER reserves the right to negotiate final Contract terms with the awarded **RESPONDENT(S)**. If negotiations with the awarded **RESPONDENT** are unsuccessful or a Contract cannot be executed within a reasonable period, **CUSTOMER** reserves the right to terminate negotiations and proceed with negotiations with another **RESPONDENT** or take any other action permitted by applicable law and this RFO.

If the RFO is awarded, **CUSTOMER** will post a Notice of Award on the Electronic State Business Daily. However, there is no guarantee that an award, any contract, or purchase order will result from this RFO.

CUSTOMER reserves the right to reject any or all Proposals, cancel, withdraw, amend, or reissue this RFO, in whole or in part, and/or

make no award if **CUSTOMER** determines that doing so is in the best interest of the State of Texas.

10.4 Best Value Determination

Consistent with Tex. Gov't Code § 2157.003 and other applicable State of Texas procurement laws, **CUSTOMER** will consider best value for the State of Texas, in addition to the evaluation criteria listed above, when selecting a **RESPONDENT**.

In determining best value, the **CUSTOMER** may consider the results of the evaluation process together with any additional factors permitted by applicable law, including, but not limited to:

- The proposal that best meets the goals and objective as stated in this RFO;
- The proposal indicates **RESPONDENT**'s ability to reliably perform the required tasks/deliverables described in this RFO;
- The **RESPONDENT**'s ability to adhere to the schedule and delivery terms (if applicable);
- **RESPONDENT**'s experience in providing services in this RFO;
- Past Vendor Performance: In accordance with Tex. Gov't Code §§ 2155.074 and 2262.055, vendor performance may be used as a factor in the award (if applicable);
- Other factors relevant to determining the best value for the state in context of this purchase (i.e., certifications/licensure, reference checks, pricing, etc.);
- The compatibility of the proposed solution with **CUSTOMER**'s existing technology environment, architecture, and operational processes;
- The ability of the proposed solution and delivery model to support future growth, modernization, scalability, maintainability, and evolving business requirements;
- The reliability, maintainability, supportability, security, and operational maturity of the proposed service delivery approach;
- **RESPONDENT**'s approach to governance, staffing, knowledge transfer, documentation, transition, and continuous improvement;
- Compliance with applicable State of Texas laws, Department of Information Resources (DIR) standards, accessibility requirements, Texas Cyber Command cybersecurity requirements, and other requirements established by this RFO;

- The proposed pricing, total cost of ownership, and overall value offered to the **CUSTOMER**; and
- Any other factors the **CUSTOMER** determines to be relevant and permissible under applicable law.

The numerical scores assigned by individual evaluators are intended to support the evaluation process and do not, by themselves, determine Contract award. Selection of the highest-scoring Proposal does not obligate **CUSTOMER** to award a Contract to that **RESPONDENT**, and **CUSTOMER** reserves the right to consider the totality of the evaluation results and other factors identified in this RFO when determining the Proposal that represents the best value to the State of Texas.

11. Terms and Conditions

Upon Contract execution, the final Contract, together with this RFO, including the RFO, any Addenda issued by the **CUSTOMER**, the successful **RESPONDENT**'s Proposal, the Pricing Proposal, and other documents expressly incorporated by reference, shall constitute the complete agreement between the **CUSTOMER** and the successful **RESPONDENT**. Applicable terms and conditions for the Contract for this RFO can be found in Attachment C, *Sample THECB Contract*.

In addition, the following terms and conditions will govern this RFO and the resulting Contract(s). These provisions supplement, but do not replace, the requirements established elsewhere in this RFO or in the Sample Contract.

Unless otherwise expressly stated, the terms and conditions established in this section shall apply throughout the RFO process and, upon Contract execution, shall become part of the resulting Contract between the **CUSTOMER** and the successful **RESPONDENT**.

11.1 Costs Incurred

RESPONDENT shall be solely responsible for all costs incurred by **RESPONDENT** for the preparation, submission, presentation, revision, or negotiations of its Proposal, including participation in interviews, demonstrations, oral presentations, or other activities requested by **CUSTOMER** during the procurement process.

Under no circumstances shall **CUSTOMER** or the State of Texas be liable for any costs incurred by **RESPONDENT** in connection with this RFO, regardless of whether a Contract is awarded.

11.2 Waiver of Errors

CUSTOMER reserves the right, to the extent permitted by applicable law and procurement requirements, to waive minor informalities, irregularities, or technicalities in a proposal.

11.3 Acceptance of Evaluation Process

By submitting a Proposal, **RESPONDENT** acknowledges that it has reviewed and understands the evaluation process described in this RFO and agrees to be bound by its terms.

RESPONDENT further acknowledges that **CUSTOMER's** evaluation of Proposals may include both objective and subjective assessments and that **CUSTOMER** retains sole discretion in determining the Proposal that provides the best value and is most advantageous to **CUSTOMER**, consistent with the evaluation criteria and applicable procurement laws.

11.4 Protest Procedures

Any protest relating to this RFO shall be submitted and resolved in accordance with procurement protest procedures established in the applicable provisions of 19 Tex. Admin. Code, Part 1, Chapter 1, Subchapter A, General Provisions, as amended.

Failure to comply with the applicable protest procedures may result in dismissal of the protest.

11.5 Public Information Act

CUSTOMER is a government agency subject to the Texas Public Information Act (PIA), Tex. Gov't Code, Chapter 552. All Proposals and other information submitted in response to this RFO are subject to public disclosure unless otherwise excepted from disclosure under applicable law. **CUSTOMER** is also required to post contracts on its public website and to provide such information to the Legislative Budget Board for posting on its public website.

Under the PIA, certain information is protected from public release. If a **RESPONDENT** believes any portion of its Proposal contains proprietary, confidential, or trade secret information that is exempt from disclosure under the PIA, the **RESPONDENT** shall:

- Clearly label each specific portion of the Proposal claimed to be exempt from disclosure;
- Cite the specific statutory exception(s) under the PIA that support the claim of confidentiality; and
- Limit confidentiality claims only to information that is legally protected from disclosure.

Blanket assertions that an entire Proposal is confidential or proprietary are not acceptable and may be disregarded by the **CUSTOMER**.

If **CUSTOMER** receives a request for disclosure of information identified as confidential or proprietary, **CUSTOMER** will process the request in accordance with the PIA, including notifying **RESPONDENT** of the process for requesting a determination from the Office of the Attorney General.

RESPONDENT is required to make any information created or exchanged with the state pursuant to the RFO or contract, and not otherwise excepted from disclosure under the PIA, available in a format that is accessible by the public at no additional charge to the state.

11.6 Retention of Proposals

All Proposals, supporting documentation, and other materials submitted in response to this RFO become the property of **CUSTOMER** upon submission and will not be returned to **RESPONDENT**.

11.7 Intellectual Property and Indemnification

By submitting a Proposal, **RESPONDENT** represents and warrants that it possesses the necessary rights, licenses, permissions, and authority for all materials included in its Proposal.

RESPONDENT shall defend, indemnify, and hold harmless **CUSTOMER**, its officers, employees, and agents from any third-party claim, demand, action, liability, or expense arising from the alleged infringement or misappropriation of any patent, copyright, trademark, trade secret, or other intellectual property right associated with materials, software, documentation, or other content supplied by **RESPONDENT** in connection with its Proposal or any resulting Contract.

VENDOR acknowledges and agrees that all **CUSTOMER**-owned intellectual property, including any applicable trademark, copyrights, logos, graphics, etc. shall remain the intellectual property of **CUSTOMER**. **VENDOR** agrees that it shall not use **CUSTOMER** trademarks and copyrights or other intellectual property, or any marks or copyrights that are confusingly similar for any other purpose. **VENDOR** agrees it shall not assert any right, license, or interest with respect to any **CUSTOMER** intellectual property. **VENDOR** further agrees that it shall not contest, attack, dispute, challenge, attempt to cancel, oppose, or seek to challenge in any manner or in any forum, **CUSTOMER**'s rights, title, and interest to the intellectual property described above.

11.8 Responsible Use of Artificial Intelligence

11.8.1 General Prohibition

VENDOR, including its employees, subcontractors, agents, affiliates, and any third-party performing Services under the Contract, shall not upload, transmit, input, process, analyze, or otherwise use **CUSTOMER** Data with any artificial intelligence (AI), generative AI platform, machine learning model, large language model (LLM), or similar AI-enabled technology without **CUSTOMER**'s prior written approval.

For purposes of this Contract, **CUSTOMER** Data includes all information, documents, records, software, source code, datasets, metadata, reports, configurations, system information, any personally identifiable information (PII), any information or data that may fit under the scope of FERPA 34 CFR § 99.3 or Tex. Educ. Code § 61.0511(l), and other materials provided by, accessed from, or created on behalf of **CUSTOMER** during the performance of the Contract, including information that has been masked, de-identified, anonymized, aggregated, or is otherwise subject to applicable privacy or confidentiality requirements.

VENDOR shall not sell or use **CUSTOMER** Data to train, improve, fine-tune, or otherwise enhance any publicly available, commercially available, or shared artificial intelligence model or service unless expressly authorized in writing by **CUSTOMER**.

11.8.2 Request for Approval

If **VENDOR** seeks authorization to use AI technologies during the term of the Contract, **VENDOR** shall submit a written request to **CUSTOMER** describing:

- The AI technology, platform, or service proposed for use.
- The intended business purpose and expected benefits.
- The categories of **CUSTOMER** Data that would be processed.
- Security, privacy, and confidentiality safeguards.
- Data retention, storage, model training, and data ownership practices.
- Risk mitigation measures.
- Any subcontractors or third-party AI providers involved in delivering the Services.

- Any proposed cross-border data transfers.

CUSTOMER may approve, deny, or condition any request at its sole discretion. Approval of one AI technology, use case, dataset, or business process shall not constitute approval for any other use.

11.8.3 Compliance Requirements

If **CUSTOMER** authorizes the use of AI technologies, **VENDOR** shall comply with all applicable federal and state laws, regulations, contractual requirements, and **CUSTOMER** policies governing:

- Information security;
- Privacy and confidentiality;
- Auditing;
- Intellectual property;
- Accessibility;
- Records retention;
- Data governance;
- Non-discrimination; and
- Any other applicable legal or regulatory requirements.

VENDOR shall remain fully responsible for the accuracy, quality, security, confidentiality, and integrity of all Services and Deliverables produced using AI technologies. Approval of the use of AI does not relieve **VENDOR** of any contractual obligations, service levels, performance standards, or compliance requirements.

11.8.4 Unauthorized Use and Remedies

Any unauthorized use of AI technologies involving **CUSTOMER** Data, or any use inconsistent with **CUSTOMER**'s written authorization, shall constitute a material breach of the Contract.

CUSTOMER reserves the right to pursue any remedies available under the Contract or applicable law, including requiring the immediate cessation of the unauthorized activity, termination of the Contract for cause, recovery of damages, injunctive relief, and any other legal or equitable remedies available.

The obligations contained in this section shall survive the expiration or termination of the Contract.

11.8.5 AI Assisted Capabilities and Tools

CUSTOMER supports **VENDOR's** responsible use of modern software engineering tools and AI-assisted capabilities throughout the software development and testing lifecycle, including code generation, code analysis, automated test generation, defect identification, accessibility validation, documentation generation, Quality Engineering, and other engineering productivity tools where appropriate. The use of such tools shall not diminish **VENDOR's** responsibility for the quality, security, maintainability, accessibility, performance, or supportability of the delivered solution. **VENDOR** shall remain fully accountable for all deliverables produced using AI-assisted tools or technologies.

11.9 Electronic and Information Resources Accessibility

VENDOR shall ensure that all Electronic and Information Resources (EIR), including software applications, websites, web applications, mobile applications, documents, reports, forms, user interfaces, training materials, multimedia content, and other technology products or services provided under the Contract are accessible to individuals with disabilities and comply with all applicable federal and state accessibility laws, regulations, and standards.

At a minimum, **VENDOR** shall comply with:

- Tex. Gov't Code, Chapter 2054, Subchapter M (Electronic and Information Resources Accessibility);
- 1 Tex. Admin. Code, Chapters 206 and 213;
- Section 508 of the Rehabilitation Act of 1973, as amended;
- The Web Content Accessibility Guidelines (WCAG) 2.1 Level AA, or any successor standard adopted by the State of Texas during the term of the Contract; and
- **CUSTOMER's** EIR Accessibility Policy, standards, procedures, and review processes.

Accessibility shall be incorporated throughout the entire system development lifecycle, including planning, design, development, testing, implementation, documentation, maintenance, and production support. **VENDOR** shall not treat accessibility as a post-development remediation activity.

VENDOR shall be responsible for ensuring that all Deliverables, enhancements, defect corrections, configuration changes, content updates, and software releases maintain compliance with applicable accessibility

requirements. Accessibility shall be considered a functional requirement for all work performed under the Contract.

Upon request, **VENDOR** shall provide documentation demonstrating accessibility compliance, including but not limited to:

- A current Accessibility Conformance Report (ACR) using the Voluntary Product Accessibility Template (VPAT), where applicable;
- Accessibility testing results;
- Documentation describing known accessibility exceptions or limitations; and
- Remediation plans and timelines for correcting identified accessibility issues.

CUSTOMER reserves the right to conduct or require independent accessibility testing and validation of any Deliverable provided under the Contract. Any accessibility deficiencies identified by **CUSTOMER** shall be corrected by **VENDOR** at no additional cost to **CUSTOMER** within timeframes established by **CUSTOMER**.

Failure to comply with applicable accessibility requirements or **CUSTOMER's** EIR Accessibility Policy may be considered a material deficiency in performance and may require remediation, withholding of Deliverable acceptance, or other contractual remedies available to **CUSTOMER**.

Submission Checklist

This checklist identifies documents that must be submitted with **RESPONDENT**'s proposal to be considered responsive. A proposal received without these required documents may be deemed nonresponsive and may not be considered for contract award.

- ☐ **Excel Pricing Proposal** (9.6)
- ☐ **Solution Proposal (PDF)**
 - Executive Summary (9.1)
 - Company References (9.2)
 - Company Experience (9.3)
 - Delivery Organization and Key Personnel (9.4)
 - Technical Proposal (9.5)
 - Exceptions to Terms and Conditions (if any) (9.7)
 - Assumptions (if any) (9.7)
 - Attachment A: Conflict of Interest Disclosure Statement
 - Attachment B: Execution of Proposal
 - Attachment E: VetHUB Subcontracting Plan
- ☐ **Vendor VetHUB Subcontracting Plan** (if applicable)

Appendix A – Glossary of Terms and Acronyms

This Appendix provides definitions for technical, operational, engineering, procurement, and other specialized terms and acronyms used throughout this RFO and any resulting Contract. This Appendix is intended to promote a common understanding of terminology used in the RFO and related Contract documents.

Glossary of Terms

The following terms have the meanings indicated below.

Algorithms: A step-by-step set of instructions or rules designed to perform a specific task or solve a problem. Algorithms process input data to produce an output for computer programming, automation, analytics, and decision-making systems.

Application Programming Interface: A defined set of protocols, specifications, endpoints, and methods that enables software applications, systems, platforms, or services to securely exchange data or invoke functionality. APIs may be used to integrate **CUSTOMER** applications with internal systems, external systems, cloud services, third-party platforms, and other technology services.

Architecture Decision Record: A concise document that captures a significant architectural or technical decision, including the alternatives considered, rationale, assumptions, dependencies, risks, and operational impacts supporting the decision.

Artificial Intelligence: Software, platforms, services, or models that perform tasks traditionally requiring human intelligence, including generative AI, machine learning, large language models, foundation models, and similar technologies capable of generating, analyzing, transforming, classifying, or making decisions based on data.

Best Value: The determination made by the **CUSTOMER**, consistent with applicable Texas procurement law, that a Proposal provides the greatest overall value to the State after consideration of the published evaluation criteria, pricing, technical merit, qualifications, lifecycle costs, and other factors permitted by law.

Blue/Green Deployment: A software deployment strategy that maintains two parallel production environments to reduce deployment risk and minimize service disruption by allowing rapid transition between production environments and immediate rollback when necessary.

Cloud Operations and Infrastructure: The administration, monitoring, configuration, automation, optimization, maintenance, and operational support of the cloud resources, application environments, platform services, and infrastructure within the scope of this Contract.

Continuous Integration/Continuous Deployment: An automated software engineering practice that integrates source code changes, performs automated builds, testing, security validation, quality checks, and controlled software deployments through release pipelines.

Contract: The written agreement executed between the **CUSTOMER** and the **VENDOR**, including all attachments, exhibits, amendments, work orders, purchase orders, and documents incorporated by reference.

CUSTOMER: The Texas Higher Education Coordinating Board, acting through its authorized representatives responsible for administering this RFO and any resulting Contract.

CUSTOMER Data: All information, documents, records, software, source code, datasets, metadata, reports, configurations, system information, and other materials provided by, accessed from, maintained for, or created on behalf of the **CUSTOMER** in connection with the Contract.

Definition of Done: The documented engineering, quality, security, accessibility, testing, documentation, and release readiness criteria that must be satisfied before software work is considered complete.

Deliverable: Any work product, document, report, software, configuration, source code, design, technical artifact, or other item the **VENDOR** is required to provide under the Contract.

Delivery Organization: The **VENDOR's** overall organizational structure, personnel, leadership, governance, technical capabilities, and supporting resources assigned or available to deliver the Services under the Contract. The Delivery Organization includes the dedicated Scrum Team(s), delivery and technical leadership, and other engineering, operational, security, quality, architecture, or specialized resources used to support delivery of the Services, whether or not such resources are assigned full-time to a Scrum Team.

DevSecOps: A software engineering methodology integrating software development, cybersecurity, and IT operations throughout the software development lifecycle through automation, security, testing, monitoring, and continuous improvement.

Family Educational Rights and Privacy Act: The federal law codified at 20 U.S.C. § 1232g and its implementing regulations at 34 C.F.R. Part 99, which protect the privacy of student education records and govern the access, use, disclosure, and safeguarding of PII contained in those records. The **VENDOR** shall comply with all applicable FERPA requirements when creating, receiving, accessing, maintaining, processing, transmitting, storing, or otherwise handling education records or PII on behalf of the **CUSTOMER**.

Generative AI: Artificial intelligence systems capable of generating new content such as text, images, audio, video, or software code based on learned patterns.

Infrastructure as Code: A software engineering practice that provisions, configures, and manages infrastructure and cloud resources through version-controlled source code and automated deployment processes.

Knowledge Management: The disciplined process of creating, organizing, maintaining, preserving, and sharing technical documentation, operational procedures, engineering knowledge, architecture artifacts, and institutional knowledge necessary to support the ongoing operation and continuous improvement of the **CUSTOMER's** technology portfolio.

Large Language Model: An artificial intelligence model trained on extensive text data to understand, generate, summarize, classify, and process natural language.

Product Owner: The **CUSTOMER** representative responsible for establishing product vision, managing and prioritizing the product backlog, clarifying business requirements, accepting completed work, and representing business priorities throughout the Agile software development lifecycle.

Proposal: The **RESPONDENT's** complete response to this RFO, including all attachments, pricing information, amendments, certifications, and supporting documentation submitted for evaluation.

Quality Engineering: A comprehensive software engineering discipline that integrates quality throughout the software development lifecycle through planning, automation, testing, code review, security validation, accessibility validation, quality metrics, and continuous improvement.

Release Management: The disciplined process of planning, coordinating, validating, approving, deploying, verifying, and stabilizing software releases within the production environment.

Release Plan: The documented implementation plan describing the scope, deployment activities, validation procedures, rollback strategy, communications, responsibilities, and operational activities for a production software release.

Release Readiness Assessment: The documented assessment confirming that all engineering, testing, security, accessibility, operational readiness, and deployment requirements have been satisfied before production deployment.

RESPONDENT: An individual or legal entity submitting a Proposal in response to this RFO.

Scope of Work: Description of the Services, Deliverables, responsibilities, and performance expectations established in this RFO and incorporated into the resulting Contract.

Scrum Team: A dedicated, cross-functional team provided by the **VENDOR** responsible for designing, developing, testing, deploying, documenting, maintaining, and supporting software using Agile delivery methodologies.

Service Level Agreement: The documented service level objectives, performance metrics, response times, resolution targets, availability requirements, and other measurable service commitments established under the Contract.

Service Transition Plan: A **CUSTOMER**-approved plan describing the activities, schedule, governance, resource assignments, knowledge transfer, operational readiness, risks, dependencies, and acceptance criteria necessary to transition Managed Services.

Services: The professional, technical, engineering, operational, maintenance, support, and related activities the **VENDOR** is required to perform under the Contract.

RFO: This RFO, including all appendices, attachments, exhibits, addenda, amendments, and documents incorporated by reference.

State: The State of Texas and its agencies, instrumentalities, officers, employees, and authorized representatives.

Technical Design Package: A comprehensive technical design document describing the proposed solution architecture, technical approach, integration impacts, security considerations, testing strategy, deployment approach, operational impacts, and implementation plan for significant technical changes.

VENDOR: The **RESPONDENT** awarded a Contract under this RFO.

Acronyms

Acronym	Definition
ACR	Accessibility Conformance Report
ADR	Architecture Decision Record
AI	Artificial Intelligence
API	Application Programming Interface
CI/CD	Continuous Integration / Continuous Deployment
DDI	Design, Development, and Implementation
DIR	Texas Department of Information Resources
DoD	Definition of Done
EIR	Electronic and Information Resources
ESBD	Electronic State Business Daily
FERPA	Family Educational Rights and Privacy Act

Acronym	Definition
HSP	VetHUB Subcontracting Plan, as applicable
IaC	Infrastructure as Code
LLM	Large Language Model
MTF	My Texas Future
NIST	National Institute of Standards and Technology
NSC	National Student Clearinghouse
PIA	Public Information Act
PII	Personally Identifiable Information
QE	Quality Engineering
RFO	Request for Offers
RRA	Release Readiness Assessment
SLA	Service Level Agreement
SMS	Support and Maintenance Services
TDP	Technical Design Package
THECB	Texas Higher Education Coordinating Board
TIN	Texas Identification Number
TX-RAMP	Texas Risk and Authorization Management Program
UX	User Experience
UI	User Interface
VPAT	Voluntary Product Accessibility Template
VetHUB	Veteran Heroes United in Business
WCAG	Web Content Accessibility Guidelines

Appendix B – Information Security Standards

Purpose

This Appendix establishes the minimum information security, cybersecurity, privacy, and data protection requirements applicable to the **VENDOR** and any subcontractors performing Services under the Contract. These standards are intended to protect the confidentiality, integrity, availability, and resilience of **CUSTOMER** Data, Information Resources, and Information Systems throughout the term of the Contract.

The requirements contained in this Appendix supplement, but do not replace, the security, privacy, and compliance obligations established elsewhere in the Contract. The **CUSTOMER** reserves the right to establish additional security requirements when necessary to protect **CUSTOMER** Data, comply with applicable laws or regulations, address emerging cybersecurity threats, or mitigate identified risks.

Definitions

For purposes of this Appendix, the following definitions apply:

Access Credentials means usernames, passwords, cryptographic keys, certificates, tokens, multifactor authentication credentials, service accounts, API keys, and other authentication mechanisms used to access **CUSTOMER** Information Resources or Information Systems.

CUSTOMER Data means all information, records, files, databases, software, source code, configuration information, metadata, documents, reports, communications, credentials, logs, backups, analytics, system information, and other information provided by, created for, maintained by, or otherwise accessible through the **CUSTOMER**, regardless of format or media. **CUSTOMER** Data includes Confidential Information, Personal Identifying Information, Sensitive Personal Information (SPI), student records protected under FERPA, and any other information protected by applicable law or **CUSTOMER** policy.

Information Resources has the meaning established by Tex. Gov't Code Chapter 2054 and includes information and information technology assets used to store, process, transmit, or manage **CUSTOMER** Data.

Information System means any application, platform, infrastructure component, cloud service, database, network, endpoint, software, or other technology resource used in support of the Services.

Security Incident means any actual or suspected event that jeopardizes the confidentiality, integrity, or availability of **CUSTOMER** Data or Information Resources, or constitutes a violation of applicable security policies, standards, or contractual requirements.

Security Breach means a confirmed unauthorized acquisition, disclosure, access, use, modification, destruction, or loss of **CUSTOMER** Data that compromises its confidentiality, integrity, or availability or otherwise requires notification under applicable federal or state law.

Unless otherwise defined herein, capitalized terms shall have the meanings assigned elsewhere in the Contract.

Information Security Requirements

The **VENDOR** shall establish, implement, maintain, and continuously improve an information security program appropriate for the nature of the Services provided under the Contract.

At a minimum, the **VENDOR** shall:

- Comply with applicable federal and state laws, regulations, and contractual requirements governing information security, privacy, and data protection.
- Comply with 1 Tex. Admin. Code, Chapter 477, Texas Cybersecurity Framework requirements, as applicable, including the Security Control Standards Catalog published under 1 Tex. Admin. Code 477.76 (or its successor catalog published by the Texas Cyber Command), which is based on NIST Special Publication 800-53, Revision 5) including the Security Control Standards Catalog published under 1 Tex. Admin. Code 477.76 (or its successor catalog published by the Texas Cyber Command), which is based on NIST Special Publication 800-53, Revision 5).
- Maintain an information security program aligned with the NIST Cybersecurity Framework (CSF) 2.0 and applicable NIST Special Publications, the DIR/Texas Cyber Command Security Control Standards Catalog (NIST SP 800-53, Rev. 5-based) and, where not otherwise specified, the NIST Cybersecurity Framework (CSF) 2.0
- Comply with all **CUSTOMER** information security policies, standards, and procedures communicated to the **VENDOR**.
- Require subcontractors performing Services under the Contract to comply with the same information security requirements applicable to the **VENDOR**. Ensure that personnel performing Services under the Contract complete a cybersecurity training program certified under Tex. Gov't Code § 2063.103, consistent with training requirements applicable to state agency contractors with access to state computer systems or databases.

Data Protection Requirements

The **VENDOR** shall protect **CUSTOMER** Data throughout its lifecycle, including its creation, collection, access, storage, transmission, processing, backup, archival, and destruction.

At a minimum, the **VENDOR** shall:

- Encrypt **CUSTOMER** Data in transit and at rest using industry-accepted cryptographic standards (FIPS 140-2 or FIPS 140-3 validated cryptographic modules, or successor federal standard).
- Store **CUSTOMER** Data only within the geographical boundaries of the United States unless otherwise approved in writing by the **CUSTOMER**.
- Prohibit the storage of **CUSTOMER** Data on removable media without prior written approval from the **CUSTOMER**.
- Use **CUSTOMER** Data solely for the purpose of performing the Services described in the Contract.
- Prevent unauthorized disclosure, alteration, destruction, or misuse of **CUSTOMER** Data.

Access Control Requirements

The **VENDOR** shall implement appropriate logical and physical access controls to ensure that only authorized individuals have access to **CUSTOMER** Data and Information Resources.

The **VENDOR** shall:

- Enforce the principle of least privilege.
- Implement role-based access controls where appropriate.
- Require multifactor authentication for privileged access and remote access.
- Use unique user accounts for all individuals accessing **CUSTOMER** Information Resources.
- Promptly disable access when personnel no longer require access or are no longer assigned to the Contract.
- Conduct periodic reviews of privileged access.

Cloud and Infrastructure Security

The **VENDOR** shall maintain appropriate administrative, technical, and physical safeguards for all cloud services, infrastructure, networks, platforms, and applications used in performance of the Contract.

These safeguards shall include:

- Secure configuration management.
- Network segmentation.
- Continuous vulnerability management.

- Security logging and monitoring.
- Secure management of encryption keys, secrets, and certificates.
- Timely application of security patches and updates.

Security Monitoring and Incident Response

The **VENDOR** shall maintain documented security monitoring and incident response capabilities appropriate for the Services provided.

The **VENDOR** shall:

- Continuously monitor Information Systems supporting **CUSTOMER** Data.
- Investigate suspected security events.
- Contain, eradicate, and recover from Security Incidents.
- Preserve evidence necessary for forensic investigation.
- Cooperate fully with the **CUSTOMER** during incident response activities.

Artificial Intelligence Requirements

The **VENDOR** shall comply with all Responsible Use of Artificial Intelligence requirements established in the Contract.

The **VENDOR** shall not process **CUSTOMER** Data using artificial intelligence technologies, including applicable requirements under the Texas Responsible Artificial Intelligence Act (TRAIGA) and any State agency AI use policies, without the **CUSTOMER**'s prior written approval and shall ensure that any authorized use complies with applicable security, privacy, confidentiality, accessibility, and data governance requirements, including disclosure of the specific AI system(s), model provider(s), data handling practices, and any subprocessors involved in the AI processing.

Data Ownership and Return

All **CUSTOMER** Data remains the exclusive property of the **CUSTOMER**.

Upon expiration or termination of the Contract, or upon request by the **CUSTOMER**, the **VENDOR** shall promptly return or securely destroy **CUSTOMER** Data in accordance with the **CUSTOMER**'s written instructions and certify completion of the return or destruction.

The **VENDOR** shall not retain **CUSTOMER** Data except as expressly authorized by law or the Contract.

Security Assessments and Right to Audit

The **CUSTOMER** reserves the right to assess the **VENDOR**'s compliance with the information security requirements established in the Contract.

Upon request, the **VENDOR** shall provide security documentation and evidence demonstrating compliance, including:

- System Security Plans.
- Security policies and standards.
- SOC 2 Type II reports or equivalent.
- TX-RAMP certification documentation, where applicable.
- Independent penetration test reports.
- Vulnerability assessment summaries.
- Network architecture diagrams.
- Data flow diagrams.
- Risk assessments.
- Security awareness training records.

The **CUSTOMER** may conduct or require independent security assessments, audits, or compliance reviews throughout the Contract term.

Security Documentation

The **VENDOR** shall maintain current security documentation supporting the Services performed under the Contract.

Documentation shall be updated as significant changes occur and shall be made available to the **CUSTOMER** upon request.

Security Incident and Breach Notification

The **VENDOR** shall notify the **CUSTOMER** immediately upon discovery of any actual or suspected Security Incident affecting **CUSTOMER** Data or Information Resources and no later than twenty-four (24) hours after discovery, to allow the **CUSTOMER** sufficient time to satisfy its own reporting obligations to the Texas Cyber Command (or successor state cybersecurity authority) under Tex. Gov't Code § 2063.302

Within seventy-two (72) hours, the **VENDOR** shall provide a written preliminary incident report describing:

- The nature of the incident.
- Systems and data affected.
- Known or suspected root cause.
- Containment actions taken.
- Planned remediation activities.

- Current operational impact.

The **VENDOR** shall cooperate fully with the **CUSTOMER** throughout the investigation, remediation, recovery, and post-incident review.

Survival

The obligations contained in this Appendix relating to confidentiality, data protection, information security, breach notification, audit rights, return or destruction of **CUSTOMER** Data, and any other provisions that by their nature should survive termination shall remain in effect following expiration or termination of the Contract until all **CUSTOMER** Data has been returned or securely destroyed and all contractual obligations have been satisfied.

Appendix C

Vendor Program (VetHUB)

The purpose of the Vendor Program (VetHUB) is to promote full business opportunities in State contracting in accordance with the goals specified by the Legislature and the Comptroller of Public Accounts. Under state law, each state agency must make a good faith effort to meet or exceed its goals and assist vendors in participating in competitive procurement opportunities. THECB is statutorily required to participate in the program and encourages all eligible vendors to participate in this RFO.

Vendor Program Subcontracting Plan

THECB has determined that subcontracting opportunities are possible in connection with this RFO. Therefore, a Vendor Program Subcontracting Plan (VPSP) is required as part of the Proposal. Respondents must submit a Vendor Program Subcontracting Plan. Questions regarding the Vendor program or Vendor Subcontracting must be submitted to THECB's Vendor Client Gateway.