CONTRACT

(fee-for-goods or services contract with an individual, business, non-profit, or governmental entity of another state)

Begin Date	End Date	Agency Tracking #	Edison Record ID
April 1, 2025	March 31, 2028	31865-00641	86067

Contractor Legal Entity Name	Edison Vendor ID
Inspira Enterprise, Inc.	0000285177

Goods or Services Caption (one line only)

Managed Security Operation Services

Contractor	Assistance Listing Number#
☒ Contractor	93.778 Dept. of Health & Human Services/Title XIX

Funding —

FY	State	Federal	Interdepartmental	Other	TOTAL Contract Amount
2025	$196,541.70	$196,541.70	$0.00	$0.00	$393,083.40
2026	$786,166.65	$786,166.65	$0.00	$0.00	$1,572,333.30
2027	$786,166.65	$786,166.65	$0.00	$0.00	$1,572,333.30
2028	$589,625.00	$589,625.00	$0.00	$0.00	$1,179,250.00
TOTAL:	**$2,358,500.00**	**$2,358,500.00**	**$0.00**	**$0.00**	**$4,717,000.00**

Contractor Ownership Characteristics:

☐ Minority Business Enterprise (MBE):

☐ African American ☐ Asian American ☐ Hispanic American ☐ Native American

☐ Woman Business Enterprise (WBE)

☐ Tennessee Service Disabled Veteran Enterprise (SDVBE)

☐ Disabled Owned Business (DSBE)

☐ Tennessee Small Business Enterprise (SBE): $10,000,000.00 averaged over a three (3) year period or employs no more than ninety-nine (99) employees.

☐ Government ☐ Non-Minority/Disadvantaged ☒ Other: For-Profit Ogranization

Selection Method & Process Summary (mark the correct response to confirm the associated summary)

☒ Competitive Selection	Request for Proposal 31865-00641
☐ Other	

Budget Officer Confirmation: There is a balance in the appropriation from which obligations hereunder are required to be paid that is not already encumbered to pay other obligations.

Crystal Allen

Digitally signed by: Crystal Allen
DN: CN = Crystal Allen email = crystal.g.allen@tn.gov C = US O = TennCare OU = Fiscal
Date: 2025.03.10 10:54:04 -05'00'

Speed Chart (optional)	Account Code (optional)

Docusign Envelope ID: 40B7BFA4-E1BB-4360-9C9C-6FA33E97F12A

CONTRACT
BETWEEN THE STATE OF TENNESSEE,
DEPARTMENT OF FINANCE AND ADMINISTRATION,
DIVISION OF TENNCARE
AND
INSPIRA ENTERPRISE, INC.

This Contract, by and between the State of Tennessee, Department of Finance and Administration, Division of TennCare ("State" or "TennCare") and Inspira Enterprise, Inc. ("Contractor"), is for the provision of Managed Security Services as further defined in the "SCOPE." State and Contractor may be referred to individually as a "Party" or collectively as the "Parties" to this Contract.

The Contractor is For-Profit Corporation
Contractor Place of Incorporation or Organization: TX
Contractor Edison Registration ID # 0000285177

A. SCOPE

A.1. The Contractor shall provide all goods or services and deliverables as required, described, and detailed below and shall meet all service and delivery timelines as specified by this Contract.

A.2. Definitions. For purposes of this Contract, definitions and abbreviations shall be as set forth in Attachment A, Definitions and Abbreviations.

A.3. The Contractor shall provide TennCare with Managed Security Services (MSS) 24 hours per day, seven days per week, 365 days per year (24x7x365 days) for the duration of the Contract to protect the confidentiality, integrity, and availability of the information and systems that support TennCare. The MSS shall incorporate current industry-standard tools and technology and shall be flexible to accommodate current trends, technological advances, industry-leading capabilities, and regulatory requirements.

A.3.1. The Contractor shall provide MSS inclusive of all hardware, software, cloud, and infrastructure costs required to acquire, install, operate, and maintain the MSS.

A.3.2. As the Contractor and its subcontractors are uniquely positioned to monitor TennCare Solution Vendor systems, the Contractor and its subcontractors shall not bid on any applicable TennCare Solution Vendor procurements nor serve as a subcontractor on a TennCare Solution Vendor contract during the Term.

A.4. The Contractor shall provide associated services and deliverables as described and detailed in this Contract and attached documents. References to specific Services, as opposed to all Services required under this Contract, may be inferred in each instance from the context of the Contract provisions.

A.4.1. The descriptions of Contractor Deliverables in this Contract do not include every possible duty, task, or intermediate Deliverable necessary to achieve success on this Contract. The Contractor shall receive written approval from TennCare for Deliverables to be effective. The Contractor shall be responsible for clarifying in writing any lack of detail it perceives in a specific area of work - or for a specific Deliverable - where it would appear to otherwise relieve the Contractor of a duty to conform with TennCare Governance Standards. This includes all intermediate steps, Deliverables, or processes reasonably necessary to achieve the desired outcome described in each section of the Contract.

A.4.2. The Contractor shall work in conjunction with TennCare and designated representative enterprise vendors, as necessary or at the request of TennCare, to coordinate and complete required activities and Deliverables.

A.4.3. Nothing in this Contract shall be deemed to be a delegation to the Contractor of the State's non-delegable duties under the TennCare program administered by the single state agency, as designated by the State and CMS, pursuant to Title XIX of the Social Security Act (42 U.S.C § 1396 *et seq.),* Section 1115 research and demonstration waiver

Docusign Envelope ID: 40B7BFA4-E1BB-4360-9C9C-6FA33E97F12A

granted to the State and any successor programs, or the Federal Children's Health Insurance Program (CHIP), known in Tennessee as "CoverKids," administered by the State pursuant to Title XXI of the Social Security Act.

A.4.4. The Contractor shall adhere to all documents located in Attachment C, Procurement Library, including any updated version of such documents that may occur during the Term, as directed by TennCare.

A.5. Phased Implementation and Operation

A.5.1. Prior to any implementation or operations engagement, the Contractor shall engage TennCare to review and approve the strategic planning and design.

A.5.2. Implementation: The Contractor shall implement the Security Operations Center (SOC) Platform that will function as a comprehensive Solution. The implemented MSS shall:

A.5.2.1. Meet the service and delivery timelines for MSS implementation as specified in Contractor's approved Project Schedule. Any variances from these timelines, for any reason and whether approved by TennCare or not, will not result in additional cost(s) to TennCare.

A.5.2.2. Meet all Functional Requirements and Non-Functional Requirements described in Sections A.3 through A.6.5 and Sections A.7 through A.13.

A.5.2.3. Comply with all applicable Service Level Agreements (SLAs) defined in Attachment B, Service Level Agreements and Liquidated Damages.

A.5.2.4. The Contractor shall be responsible for all data exchanges between agreed upon environments throughout implementation at no additional cost to TennCare.

A.5.2.4.1. The Contractor shall design and implement components for data exchanges to be secured and cost effective so that TennCare shall not incur any additional cost.

A.5.3. Operations and Maintenance (O&M) Phase

A.5.3.1. At the conclusion of the MSS Implementation Phase, the Contractor shall operate the MSS as required by the O&M Phase, defined in Sections A.11.6.

A.5.3.2. The Contractor shall be responsible for all data exchanges between agreed upon environments throughout the O&M Phase at no additional cost to TennCare.

A.5.3.2.1. The Contractor shall design components for data exchanges that meet required security protocols be cost-effective so that TennCare shall not incur any additional costs.

A.6. Managed Security Operations Center Services (MSOCS) Requirements

A.6.1. Security Information and Event Management (SIEM)

A.6.1.1. The Contractor shall provide security information and event management services to TennCare.

A.6.1.2. The Contractor shall utilize TennCare's current SIEM-User Interface (UI) and other TennCare tools to perform searches for Contractor's investigation.

A.6.1.3. The Contractor shall develop and deploy up to twenty (20) new and enhanced SIEM use cases each year of the Contract.

A.6.1.4. The Contractor shall recommend SIEM use cases and provide evidence and additional technical and business justification for the recommended use cases to TennCare.

A.6.1.5. The Contractor shall perform content implementation and conduct Unit Testing, Quality Assurance Testing and User Acceptance Testing.

Docusign Envelope ID: 40B7BFA4-E1BB-4360-9C9C-6FA33E97F12A

A.6.1.6. The Contractor shall develop and update Standard Operations Procedures (SOP) documents within five (5) Business Days for each use case the Contractor develops, updates, enhances, or tunes.

A.6.1.7. The Contractor shall provide evidence to TennCare and the SIEM Engineering Team of SIEM parsing issues within two (2) hours of discovery and work collaboratively to resolve the issues.

A.6.1.8. The Contractor shall ensure all log sources are operational and report issues to the SIEM Engineering Team within thirty (30) minutes of discovery through a ServiceNow ticket when a log source/application is not available or not working as expected in the SIEM.

A.6.1.9. The Contractor shall work with the SIEM Engineering Team to onboard additional log sources or applications as requested by TennCare.

A.6.1.10. The Contractor shall ensure all use cases are operational and work with the SIEM Engineering Team to resolve any issues with the alerting in accordance with established Service Level Agreements in Attachment B, Service Level Agreements and Liquidated Damages.

A.6.1.11. The Contractor shall provide recommendations to TennCare for any enhancements/changes to the SIEM that will enhance TennCare's security posture.

A.6.1.12. The Contractor shall develop or modify dashboards and reports as requested in writing by TennCare.

A.6.1.13. The Contractor shall recommend use case tuning using the monthly False Positive Ticket Reports described in section A.6.5.1.2 or as requested by TennCare. Tuning includes adjusting rules logic and thresholds as applicable.

A.6.1.14. The Contractor shall review the criticality of use cases, at a minimum quarterly, and work collaboratively with TennCare to assign a new criticality based on the review results.

A.6.2. Threat Intelligence

A.6.2.1. The Contractor's program shall integrate with TennCare's current SIEM.

A.6.2.2. The Contractor shall maintain active subscriptions to at least three (3) Threat Intelligence Services using the STIX\TAXII format for integration with SIEM (Security Information and Event Management) and SOAR (Security Orchestration, Automation, and Response). Two (2) of the three (3) sources must be MS-ISAC and Threat Connect. The one (1) other Threat Intel Services must be agreed upon with TennCare before implementation.

A.6.2.3. The Contractor shall utilize TennCare approved Open-Source Threat Intelligence to gather intelligence on active threats that are relevant to TennCare no less than twice within each twenty-four (24)-hour period. Threat Intelligence must be gathered from various sources, ranging from public sources, technical sources, dark web & deep web, underground forums, special access sites, code repositories, paste bin, and human analyst.

A.6.2.4. The Contractor shall process Indicators of Compromise (IOCs) in the environment to verify if TennCare systems are affected by any of the latest active threats and provide remediation recommendations to TennCare within one (1) hour of discovery. The IOC's shall be ranked with a reliability score, detection quality, or risk score. Scores must be justified with the rationale behind the given scores. Scores must be dynamic to represent the automated real-time risk of the IOC.

Docusign Envelope ID: 40B7BFA4-E1BB-4360-9C9C-6FA33E97F12A

A.6.2.5. The Threat Intelligence feeds such as MS-ISAC shall identify new global threats around the globe as Malicious IP Addresses, Domain, URLs, Filename, File hash, Email addresses, Known C&C (Command and Control) hosts, Geolocation feeds like Lat long, ISP, Country, etc.

A.6.2.6. The collection of Threat Intelligence from various sources shall be automated and allow mass collection of intelligence with low false positives in real-time.

A.6.2.7. The Contractor's services shall include threat briefings that include the latest threats that are relevant to TennCare, search results for IOCs, and actions taken by analysts. The Contractor shall provide background on attacks, attack vectors, and kill chain methodology. The frequency of this report shall be bi-weekly at a minimum, unless otherwise agreed upon in writing between TennCare and the Contractor.

A.6.2.8. The Contractor shall monitor the Dark Web for the information and documents related to TennCare and share the data with TennCare daily in an automated manner.

A.6.2.9. The Contractor shall support, train, guide, and coach TennCare staff on the usage and quality of Threat Intelligence feeds.

A.6.2.10. The Contractor shall publish actionable intelligence alerts to TennCare analysts for defined use cases (e.g., compromised credentials and IOC associated with active malicious campaigns)

A.6.2.11. The Contractor shall publish situational awareness alerts to TennCare analysts for use cases (e.g., New security threats under consideration that could impact the business)

A.6.2.12. The Contractor's solution must be able to create, monitor, and automate alerts and reports for threats on the Dark Web, including, but not limited to, the following:

A.6.2.12.1. Employee or member compromised credentials.

A.6.2.12.2. Sensitive information Leakage such as Username Password Secret token access keys

A.6.2.12.3. Compromised PII such as Email ID , Phone number and Address

A.6.2.12.4. Exposed Cloud infrastructure or storage

A.6.2.12.5. Malware and Malicious Infrastructure related to the tn.gov domain

A.6.2.12.6. Private / Sensitive Documents relating to TennCare

A.6.2.12.7. Hacking documents/tools specifically targeting TennCare

A.6.2.12.8. Leaked Source Code

A.6.2.12.9. Intellectual property exposed or leaked

A.6.2.12.10. Technical Information / Data that could be used to compromise TennCare systems

A.6.2.12.11. Mentions of IP Addresses and Infrastructure

A.6.2.12.12. Mentions of executives

A.6.3. Incident Response

A.6.3.1. The Contractor shall operate the Security Operations Center (SOC) 24 hours a day, 7 days a week (24x7), 365 days a year (24x7x365) for the duration of the Term.

Docusign Envelope ID: 40B7BFA4-E1BB-4360-9C9C-6FA33E97F12A

A.6.3.2. The Contractor shall monitor security events throughout TennCare's on-premises network and cloud environments by analyzing logs from servers, network devices, databases, firewalls, Virtual Private Network (VPNs), Web Application Firewall (WAFs), endpoints, Internet of Things (IoT) devices, and all onboarded applications, with exclusion to the systems and networks that STS manages, unless provided.

A.6.3.3. The Contractor shall perform 7 days a week (24x7) monitoring to detect malicious events and escalate to TennCare in accordance with the SLAs in Attachment B, Service Level Agreements and Liquidated Damages.

A.6.3.4. The Contractor shall monitor security incidents through all phases of the incident response process and provide support to TennCare as requested.

A.6.3.5. The Contractor shall perform real-time monitoring, event triage, analysis, threat intel correlation, investigation, remediation recommendation, containment, escalation, and ticket enrichment capabilities.

A.6.3.6. The Contractor shall initiate an Incident ticket in TennCare ticketing system upon discovery of a suspected/confirmed security event or breach in accordance with the SLAs in Attachment B, Service Level Agreements and Liquidated Damages.

A.6.3.7. The Contractor shall maintain accurate TennCare emergency contact information to contact in case of an emergency situation (breach or security incident).

A.6.3.8. The Contractor shall collaborate with all necessary stakeholders and third parties as directed by TennCare.

A.6.3.9. The Contractor shall participate in all Incident Response tabletop exercises as requested by TennCare.

A.6.3.10. Beginning the second year of Term on a date determined by TennCare, the Contractor shall hunt for threats, including zero-day threats, within the TennCare environment, identify threats, and provide mitigation/remediation recommendations to TennCare.

A.6.3.11. The Contractor shall notify TennCare within one (1) hour of discovery of a suspected or actual system or data breach of Contractor's environment.

A.6.3.12. The L1 and L2 staff shall assist the L3 analyst with digital forensic analysis on an as-needed basis or as directed by TennCare.

A.6.3.13. Ticketing System

A.6.3.13.1. The Contractor shall utilize an ITSM (IT Service Management) system which must interface with the TennCare ticketing system to facilitate TennCare workflows.

A.6.4. Automation

A.6.4.1. The Contractor shall recommend new playbook requirements for the TennCare SOAR platform:

A.6.4.1.1. The Contractor shall define the logic to develop the playbooks.

A.6.4.1.2. The Contractor shall work with SIEM Engineering team to implement the playbooks.

A.6.4.2. The Contractor shall create requests in the State's approved ITSM tool for development of playbooks in SOAR platform.

A.6.4.3. The Contractor shall work with the SIEM Engineering Team to modify existing SOAR playbooks as needed or as requested by TennCare.

Docusign Envelope ID: 40B7BFA4-E1BB-4360-9C9C-6FA33E97F12A

A.6.5. Reporting

A.6.5.1. Standard Reports

A.6.5.1.1. The Contractor shall provide TennCare with a daily Threat Intelligence report including latest threats that are relevant to TennCare, search results for IOCs, and actions taken by analysts.

A.6.5.1.2. The Contractor shall provide TennCare with bi-weekly False Positive Ticket Reports to track the number of false positive tickets.

A.6.5.1.3. The Contractor shall provide TennCare with a monthly SLA Compliance report with current month metrics and rolling twelve (12) months metrics by the 3rd Business Day of each new month.

A.6.5.1.4. The Contractor shall provide TennCare with a monthly SIEM Content Pipeline Report as defined by TennCare on the current status of use case development, application onboarding and planned activities for the subsequent month no later than 3rd Business Day of each month.

A.6.5.1.5. The Contractor shall provide TennCare with a monthly Alert Matrix Report as defined by TennCare to track the current use cases that are enabled in TennCare's SIEM instances and planned activities for the subsequent month.

A.6.5.1.6. The Contractor shall provide TennCare with an Incident report to TennCare for major incidents with incident summary, comprehensive details on the findings and remediation steps taken, root cause analysis and recommendations for future Solution hardening on a cadence to be defined by TennCare.

A.6.5.1.7. The Contractor shall provide TennCare with quarterly Business Report as defined by TennCare.

A.6.5.2. Additional Reporting

A.6.5.2.1. Beginning the second year of Term on a date determined by TennCare, the Contractor shall send weekly Threat Hunting Reports detailing the Contractor's threat hunting activities and results.

A.6.5.2.2. The Contractor shall provide User and Entity Behavior Analytics (UEBA) including, but not limited to, identifying, triaging, and alerting on privileged account abuse, privilege escalation, data exfiltration, anomalous behavior, and credential compromise, in a format and cadence to be defined by TennCare.

A.6.5.3. Standard Operating Procedure Manual

A.6.5.3.1. The Contractor shall develop and maintain written policies, procedures, and standards of conduct that articulate the Contractor's commitment to comply with all applicable TennCare and Federal standards for the prevention, detection, and reporting of incidents of potentially suspicious or questionable activity, fraud, and abuse by Members, Providers, subcontractors, the Contractor, or external entities.

A.6.5.3.1.1. The Contractor shall share developed policies, procedures, and standards of conduct documents to TennCare for approval in a frequency and cadence defined by TennCare.

A.6.5.3.2. The Contractor shall refer to the TennCare IT Service Management (ITSM) Standard and TennCare IT Service Management RACI in Attachment C, Procurement Library, to develop all the ITSM processes, activities, and tasks required for ITSM in this Section A.11.10. and document the required

Docusign Envelope ID: 40B7BFA4-E1BB-4360-9C9C-6FA33E97F12A

ITSM procedures in the Standard Operating Procedures (SOP) Manual for TennCare approval.

A.6.5.3.3. The Contractor shall follow and execute all procedures and processes required for the MSS Solution in the approved SOP Manual.

A.6.5.3.4. The Contractor shall build and maintain a detailed SOP Manual for the MSS Solution for the purposes of easily onboarding new resources and consistent operation of the MSS Solution. The SOP Manual shall also be made available to TennCare with CISO approval. TennCare may require a SOP Manual to be written for specific system support functions. The Contractor shall provide any and all tools necessary to fulfil the SOP Manual obligations related to executing these capabilities.

A.6.5.3.5. The Contractor shall incorporate the outcomes and recommendations of the Continuous Improvement Process (CIP) into SOP Manual updates.

A.6.5.3.6. The Contractor shall maintain the SOP as the document of record for MSS Solution activities, maintain the SOP under Configuration Management control, and update SOP documentation as a standard part of the change management process.

A.7. Data Governance

A.7.1. The Contractor shall support TennCare's policies and procedures to promote data documentation, development, and management of defined data entities, attributes, Data Models, and relationships to sufficiently convey the overall meaning and use of confidential data and information in accordance with the TennCare Data Governance standards, as defined by TennCare Data Policies and Standards.

A.7.2. The MSS shall prevent unauthorized access, use, abuse, disclosure, disruption, or modification of data without TennCare consent.

A.8. Hosting Requirements

A.8.1. All MSS tools or resources hosted in a public cloud environment shall be FedRAMP Moderate compliant.

A.8.2. The MSS shall include all environments necessary to develop and test changes to the MSS platform and to support the testing of the MSS as approved by TennCare.

A.8.3. The MSS shall support both DNS name-based whitelisting as well as IP based.

A.8.4. The Contractor shall communicate in writing to TennCare the overall approach to cloud hosting, including systems and operations under the auspices of subcontractors, at the request of TennCare.

A.8.5. The Contractor shall provide TennCare with access and complete visibility into the Solution's dedicated cloud account. The Contractor shall generate reports to provide to TennCare on a TennCare determined as-needed basis that track at a minimum the following, including, but not limited to, the usage and spending across projects, applications, and cost centers.

A.8.6. The Contractor shall create, based on TennCare review and approval, the organizational structure and related cloud accounts for TennCare.

A.8.7. The Contractor shall identify account owners to create the administrators specific to the TennCare account.

A.8.8. If the MSS is native to or currently implemented in a particular commercial cloud, the Contractor shall procure a dedicated cloud account for the TennCare Solution, at no additional cost to TennCare. If the Contractor deploys to a State-owned Cloud offering, the Contractor shall assume all costs associated with the deployment and operations as part of the Maximum Liability to this Contract.

Docusign Envelope ID: 40B7BFA4-E1BB-4360-9C9C-6FA33E97F12A

A.8.9. The Contractor shall optimize cloud consumption costs in the system design of cloud infrastructure and, on an ongoing basis, evaluate and optimize the configuration and architecture of compute resources in order to minimize costs.

A.8.10. The Contractor shall work with TennCare to agree on a patching schedule and frequency that meets the requirements defined in the Enterprise Information Security Policies (Section E.11.b.1); exceptions to the agreed upon schedule shall be approved by TennCare.

A.8.11. The Contractor shall support any cut-over activities of the existing functionality related to the MSS, including, but not limited to, a one-time load (conversion) of data per the TennCare Data Conversion/Management Plan, located in the TennCare Conversion Standard in Attachment C, Procurement Library.

A.9. Additional Requirements

A.9.1. The Contractor shall designate a staff member to be responsible for Contractor's electronic and information technology accessibility compliance activities to be performed under this Contract. The name and contact information for this individual shall be provided to TennCare's Office of Civil Rights Compliance (OCRC) within ten (10) days of the implementation phase of this Contract and within ten (10) days of this position being reassigned to another staff member, including reassignment due to vacancy.

A.9.2. The Contractor shall ensure average alert response times are within application SLAs defined in Attachment B, Service Level Agreements and Liquidated Damages, excluding scheduled downtime, natural disasters, and force majeure, or as agreed to in the Contract.

A.9.3. The Contractor shall comply with the TennCare's Enterprise-Wide governance policies and processes defined and approved by TennCare, located in Attachment C, Procurement Library.

A.9.4. All communication including, but not limited to, TennCare confidential, PHI, PII, or where protected data is present, shall be kept within TennCare approved communication pathways, including collaboration tools, email, and more.

A.10. Security and Privacy

A.10.1. The Contractor and all sub-contractors shall complete the TennCare information security and privacy training program and submit compliance reports to the TennCare Privacy Officer prior to their accessing TennCare information systems.

A.10.2. The Contractor shall notify the TennCare Security and Privacy office within ten (10) Business Days of suggested material changes to the requirements and deliverables within this Contract. The Contractor shall provide notification in a written email format to the TennCare Security and Privacy office for review and consideration.

A.10.3. The Contractor and all sub-contractors shall complete the TennCare information security and privacy training program regarding the accessing, disclosing, and securing FTI and submit compliance reports to the TennCare Privacy Officer prior to their accessing TennCare information systems containing FTI.

A.10.4. The Contractor and all sub-contractors shall review and sign the current version of the TennCare Acceptable Use Policy (AUP) prior to accessing TennCare network and/or data and annually thereafter.

A.10.5. The Contractor shall protect access to Sensitive Data, such as PHI, PII, and FTI from loss through the design, documentation, development, implementation, operation, and maintenance of security controls over the access to that data in accordance with MARS-E (current version) and IRS Pub 1075 (current version).

A.10.6. The Contractor shall comply with MARS-E (current version), IRS Pub 1075 (current version), HIPAA, 42 U.S.C. § 1320d and any applicable State confidentially

Docusign Envelope ID: 40B7BFA4-E1BB-4360-9C9C-6FA33E97F12A

requirements and standards regarding the collection, maintenance, use, and the protection from data loss of PHI, PII and FTI.

A.10.7. The Contractor shall certify that FTI processed during the performance of the contract shall be completely purged from all physical and electronic data storage in accordance with TennCare data retention policies and with no output retained by the Contractor at the time the work is completed. If immediate purging of physical and electronic data storage is not possible, the Contractor shall certify that any FTI in physical or electronic storage shall remain safeguarded to prevent unauthorized disclosures until all is purged.

A.10.8. The Contractor shall ensure the configuration of secure log data and event collection mechanisms is in accordance with MARS-E (current version) and IRS Pub 1075 (current version). This includes, at a minimum, the end-to-end process from log data collection, event generation, transmission, storage, and disposal.

A.10.9. The Contractor shall retain security, application, system audit, and event logs per MARS-E (current version) and TennCare retention requirements (current version) and in a format and structure that is approved by TennCare.

A.10.10. The Contractor shall ensure access to information systems is authorized based on the least privilege principal.

A.10.11. The Contractor shall track disclosures of PHI and PII and provide TennCare reports on the disclosures. These disclosure reports shall be provided to TennCare within the time limits mandated per the TennCare Privacy Program Policy and Plan.

A.10.12. The Contractor shall develop written policies, procedures, and standards of conduct for TennCare's approval, that articulate the Contractor's commitment to comply with all applicable TennCare and Federal standards for the prevention, detection, and reporting of incidents of potentially suspicious or questionable activity, fraud, and abuse by members, providers, subcontractors, the Contractor, or external entities.

A.10.13. The Contractor shall develop, maintain, and test and submit to TennCare an Incident Response Plan (IRP) and RACI with key partner roles both internal and external annually in accordance with NIST 800-61 (current version) and comply with all applicable Federal, State and TennCare breach notification laws and policies. The Contractor shall create and submit compliance and regulatory reports in accordance with Federal, State, and TennCare requirements regarding security-related events and incidents while working with TennCare towards security recovery actions.

A.10.14. The Contractor shall ensure that TennCare data is always transmitted and stored within secured cloud regions and zones that are within the Continental United States (CONUS).

A.10.15. The Contractor shall ensure that all hardware, software, tools, and networks used to support TennCare are within the CONUS.

A.10.16. The Contractor shall ensure Data Loss Prevention and Data Mining activities are in accordance with MARS-E (current version) and IRS Pub 1075 (current version).

A.10.17. The Contractor shall implement and manage technical safeguards and physical controls that prevent the unauthorized access to, use of, or tampering with TennCare computer, data or information systems in compliance with MARS-E (current version) and IRS Pub 1075 requirements (current version).

A.10.18. In the event of a breach that compromises or is suspected to compromise the confidentiality, integrity, or availability of TennCare data, the Contractor shall collaborate with the TennCare Security Team to respond to and triage the event. The TennCare Security Team shall be notified of any incident or breach of TennCare in accordance with these Contract terms and Attachment B, Service Level Agreements and Liquidated Damages.

Docusign Envelope ID: 40B7BFA4-E1BB-4360-9C9C-6FA33E97F12A

A.10.19. The Contractor shall participate in internal and 3rd party audit activities and risk assessments and provide TennCare with or assist in the preparation of any documentation required by TennCare and/or any regulatory bodies within the required time frames.

A.10.20. The Contractor shall provide TennCare with written evidence of findings (defects, vulnerabilities, errors, gaps, weaknesses, and omissions) and their planned remediation in a Plan of Action and Milestone report (POA&M), maintained monthly, until all findings are resolved.

A.10.21. The Contractor shall not permit user credentials to be transmitted in clear text.

A.10.22. The Contractor shall maintain a list of all employees and subcontractors who have access to Social Security Administration (SSA) data. The Contractor shall ensure that a current list of all employees and subcontractors who have access to SSA data is provided to TennCare on a weekly basis.

A.10.23. The contractor shall notify the TennCare Privacy and Security Offices in the event of a Security or Privacy Incident immediately upon recognition.

A.10.23.1. Notification shall be in writing made by email/fax, certified mail, or overnight parcel upon becoming aware of the event, with supplemental notification by facsimile and/or telephone as soon as practicable, to:

TennCare Privacy Office
310 Great Circle Rd.
Nashville Tennessee 37243
Phone: 615-806-6559
Facsimile: (615) 734-5289
Email: Privacy.Tenncare@tn.gov

TennCare Security Office
310 Great Circle Rd.
Nashville Tennessee 37243
Phone and Preferred Method of Contact: 615-806-6559
Facsimile: (615) 734-5289
Email: tenncare.security@tn.gov

A.11. Solutions Implementation Lifecycle (SILC) Requirements

A.11.1. The Contractor shall follow TennCare's SILC as described in the MSS TennCare Solution Implementation Lifecycle (SILC) Standard located in Attachment C, Procurement Library. The TennCare Solution Implementation Lifecycle (SILC) Standard defines TennCare's standard phased approach to solution implementation projects, details the TennCare Gate Review Process, outlines the requirement entry and exit criteria, and aligns the associated Deliverable for each Gate in the lifecycle for contractors partnering with TennCare.

A.11.2. The Contractor shall complete the required Deliverables as described in the TennCare Solution Implementation Lifecycle and defined in the MSS TennCare Solution Implementation Lifecycle RACI and Deliverables located in Attachment C, Procurement Library. The MSS TennCare Solution Implementation Lifecycle RACI and Deliverables defines the activities and Deliverables the Contractor is required to submit to TennCare for approval in order to pass the associated Gate Review.

A.11.3. The Contractor shall integrate the approved Project Schedule within the Integrated Master Schedule managed by the Strategic Project Management Office (SPMO) in accordance with the TennCare Project Management Plan Standard located in Attachment C, Procurement Library.

A.11.4. The Contractor shall complete the activities and Deliverables assigned to Contractor in the solutions RACI table based on the identified role (noted as "A", "C", "I", or "R").

Docusign Envelope ID: 40B7BFA4-E1BB-4360-9C9C-6FA33E97F12A

A.11.5. The Contractor shall submit all enhancements, upgrades, deployments, SDLC, and release management to TennCare for review, and receive written approval prior to communication of delivery commitments where data, hosting, infrastructure and contractor IS services are involved.

A.11.6. Implementation Phase

A.11.6.1. The Contractor shall complete the activities and Deliverables in the "Phases and Activities Overview" tab of the MSS TennCare Solution Implementation Lifecycle RACI and Deliverables (refer to Appendix B of the TennCare Solution Implementation Lifecycle for role definitions) for the Implementation of the MSS Solution.

A.11.6.2. All required Deliverables shall be submitted to TennCare and approved according to the Deliverable's Review Cycle as defined in the "Deliverable Definition" tab of the TennCare Solution Implementation Lifecycle RACI and Deliverables, located in Attachment C, Procurement Library. If Deliverables do not have a defined Review Cycle in column I of the "Deliverable Definition" tab, TennCare shall designate each Deliverable's classification at the start of the phase in which the Deliverable is to be completed.

A.11.7. Operations & Maintenance (O&M) Phase

A.11.7.1. The Contractor shall complete the activities and Deliverables in the "Phases and Activities Overview" tab of the MSS TennCare Solution Implementation Lifecycle RACI and Deliverables (refer to Appendix B of the TennCare Solution Implementation Lifecycle for role definitions) for O&M of the MSS Solution.

A.11.7.2. All required Deliverables must be submitted to TennCare and approved according to the Deliverable's Review Cycle defined in the "Deliverable Definition" tab of the TennCare Solution Implementation Lifecycle RACI and Deliverables, located in Attachment C, Procurement Library. If the Deliverable does not have a defined Review Cycle in column I of the "Deliverable Definition" tab, TennCare shall designate each Deliverable(s) classification at the start of the phase in which the Deliverable is to be completed.

A.11.8. Project Document Management

A.11.8.1. The Contractor shall store project documents in an online document library identified by TennCare. Project documentation includes, but is not limited to, Deliverables, Artifacts, work plans, status reports, status meeting agenda, and minutes.

A.11.8.2. The Contractor shall provide an electronic documentation format that facilitates efficient, effective, and expedited updating and dissemination of new or modified data.

A.11.8.3. The Contractor shall provide a process to update the electronic versions of project documentation. Each version shall have:

A.11.8.3.1. All pages numbered within each section;

A.11.8.3.2. A new revision date on each page; and

A.11.8.3.3. All revisions clearly identified.

A.11.8.4. The Contractor shall provide online hyperlinks to documents referenced within a Deliverable/Artifact, including Medicaid and non-Medicaid policy origination documents managed by TennCare and the Contractor within the project document library.

A.11.8.5. The Contractor shall adhere to the principle of least privileges and limit access to documentation that contains specific IP addresses, server names, node IDs,

Docusign Envelope ID: 40B7BFA4-E1BB-4360-9C9C-6FA33E97F12A

or other technical information that could compromise the security of the MSS Solution to the level required for performance of necessary activities.

A.11.8.6. The Contractor shall categorize documentation by data classification, as defined by TennCare, and securely store sensitive technical documentation as approved by TennCare.

A.11.8.7. The Contractor shall include a reference to Tennessee Code Annotated (TCA) §10-7-504 where appropriate for sensitive and confidential technical documentation.

A.11.9. Deliverable Management

A.11.9.1. The Contractor shall adhere to all Quality Management Standards provided in TennCare's Project Management Plan Standard located in Attachment C, Procurement Library.

A.11.9.2. The Contractor shall ensure that deliverables do not contain any protected Sensitive Data.

A.11.9.3. The Contractor shall handle identified Deliverables that require ad hoc updates or are updated periodically during the course of the implementation as follows:

A.11.9.3.1. The Contractor shall update content in the original Deliverable. Updated content provided in a deliverable amendment, and not integrated into the original deliverable, requires prior authorization by TennCare.

A.11.9.3.2. The Contractor's completion of, and TennCare's Acceptance of, a Deliverable during one (1) Gate Review shall be subject to the approval of TennCare and shall not constitute Acceptance of that Deliverable by TennCare for any subsequent Gate Review.

A.11.9.4. At a minimum, the Contractor shall submit a Deliverable Expectation Document (DED) to TennCare for each Deliverable at least twenty (20) Business Days prior to the submission of the original Deliverable or on an alternate timeline pre-approved in writing by TennCare.

A.11.9.5. The Contractor shall create Deliverables as defined in each approved Deliverable's DED.

A.11.9.6. The Contractor shall facilitate, for each Deliverable, a minimum of one (1) walkthrough with TennCare at least one (1) week prior to the Deliverable submission date or on a timeline preapproved by TennCare.

A.11.9.7. The Contractor shall submit, for each Deliverable, a first submission on the agreed submission date, and the Contractor shall allow TennCare to review and provide responses.

A.11.9.8. The Contractor shall submit, for each Deliverable, a subsequent submission, as specified in Table 1: Deliverable Review Cycles, resolving comments received from TennCare on the previous submission and allowing TennCare to review and provide responses based on the Project Schedule (PS).

A.11.9.9. The Contractor shall resolve all outstanding responses from TennCare prior to each Deliverable's final submission based on the Project Schedule (PS).

A.11.9.10. The Contractor shall establish and maintain data integration, exchange, and interface documentation in alignment with TennCare Enterprise Architecture Framework Standard located in Attachment C, Procurement Library.

A.11.9.11. The Contractor shall follow the review and response times based on the complexity level bucket assigned to the Deliverable in the Table of Deliverables (Section A.13), and the TennCare Solution Implementation Lifecycle RACI located in Attachment C, Procurement Library, as follows:

Docusign Envelope ID: 40B7BFA4-E1BB-4360-9C9C-6FA33E97F12A

Table 1: Deliverable Review Cycles

Deliverable Classification	Length of State Review Period for each Review Cycle	Length of Contractor Update Period after Receiving State Updates
Type A	Seven (7) Business Days	Seven (7) Business Days
Type B	Ten (10) Business Days	Ten (10) Business Days
Type C	Twenty (20) Business Days	Twenty (20) Business Days
Type D	Forty-Five (45) Business Days	Forty-Five (45) Business Days

A.11.10. Test Management

A.11.10.1. The Contractor shall ensure testing meets TennCare's Functional Requirements and Non-Functional Requirements, including integration with other TennCare systems.

A.11.10.2. The Contractor shall prepare a Test Management Plan for the MSS Solution and ensure that TennCare approves in writing the proposed testing methods, schedule, personnel, training, collaboration approach, test cases, data, environment, tools, tracking, metrics, and methods for Defect management and regression testing.

A.11.10.3. The Contractor shall receive written authorization from TennCare for the use of real data for testing.

A.11.10.4. The Contractor shall be responsible for three (3) stages of testing before Go-Live and shall provide evidence of their completion in the following Deliverables:

A.11.10.4.1. System Integration Test Report.

A.11.10.5. The Contractor shall perform Regression Testing based on solution or other system changes.

A.11.10.6. The Contractor shall participate in and support User Acceptance Testing (UAT) for Configuration Items (CIs) during Implementation and O&M, which includes creating UAT test cases, providing subject matter expert resources throughout UAT execution, and assisting planning test cycles and executing batch and real-time processes to support test case execution. All UAT activities are subject to TennCare oversight and approval.

A.11.11. MSS Support Team

A.11.11.1. The Contractor shall provide twenty-four (24) hours per day x seven (7) days per week x three hundred sixty-five (365) days per year production support to coordinate service issue identification, investigation, and diagnosis in cooperation with TennCare.

A.11.11.2. The Contractor shall have staff on-call and available outside of normal business hours as required to maintain in compliance with the TennCare SLAs defined in Attachment B, Service Level Agreements and Liquidated Damages.

A.11.11.3. The Contractor shall utilize the TennCare-approved ITSM tool to provide MSS support services for the TennCare and record and manage service-related activities.

Docusign Envelope ID: 40B7BFA4-E1BB-4360-9C9C-6FA33E97F12A

A.11.11.4. The Contractor shall manage and track all MSS related ITSM Incidents to resolution in TennCare's approved ITSM tool (e.g. ServiceNow) and provide recurring status updates in coordination with the IS Contractor ITSM reporting tool or upon request from TennCare.

A.11.11.5. The Contractor shall adhere to TennCare-approved multi-tiered support structure and escalation procedures that include security Incident Management and critical Problem (e.g., system outage) processes.

A.11.11.5.1. The IS Contractor shall provide front-line Service Desk support that accounts for Tier I Service Desk support consisting of services to address general issues and routing of higher complexity issues requiring Tier II Level Support to the appropriate MSS Support Team(s).

A.11.11.6. The Contractor shall provide Tier II Level Support, consisting of support services that require technical resources who have specialized skills related to MSS.

A.11.11.7. The Contractor shall provide Tier III Level Support requiring technical expertise related to MSS.

A.11.11.8. The Contractor shall be responsible for consolidation tracking of Tier II and Tier III Incidents to resolution in coordination with the IS Contractor, reporting to TennCare, and informing MMPVP of CI(s) changes that impact TennCare activities.

A.11.11.9. The Contractor shall be responsible for reporting the resolution results to the Tier I Service Desk.

A.11.11.10. The Contractor shall leverage TennCare's enterprise call solution to support Incident Management and resolution activities in coordination with the IS Contractor.

A.11.11.11. Reserved.

A.11.11.12. The Contractor shall develop an Incident priority matrix for MSS Support Team Incident Management activities subject to TennCare approval.

A.11.11.13. The Contractor shall implement bi-directional integrations and associated transformation mapping between the Contractor's Incident Management system and TennCare's ITSM system in collaboration with TennCare, the IS Contractor, and MMPVP.

A.11.11.14. The Contractor shall integrate Contractor's Governance Risk and Compliance (GRC) tools with the TennCare approved ITSM tool to support tracking and resolution of all GRC related vulnerabilities. The Contractor may use TennCare GRC tools identified in the TennCare Preferred Technology Standard or Contractor's own GRC tools for this purpose with TennCare approval.

A.11.11.15. The Contractor shall provide reoccurring status updates on GRC activities in coordination with the IS Contractor on a timeline defined by TennCare.

A.11.11.16. The Contractor shall monitor the production environment twenty-four (24) hours per day x seven (7) days per week x three hundred sixty-five (365) days per year and develop, maintain, and manage a plan to monitor every operation that affects the MSS Solution and associated CIs (e.g. network, software, interfaces, services, data manipulation).

A.11.11.17. The Contractor shall comply with the requirements of the ITSM Standard for additional service management functions, processes, and activities.

Docusign Envelope ID: 40B7BFA4-E1BB-4360-9C9C-6FA33E97F12A

A.11.12. Continuous Improvement Process (CIP)

A.11.12.1. The Contractor shall be responsible for managing a Continuous Improvement Process (CIP) to include repeatable, defined, and efficient management processes for optimization of MSS Solution-related Services throughout the entire Service Lifecycle.

A.11.12.2. The Contractor shall manage the CIP with TennCare-designated Key Personnel resources.

A.11.12.3. The Contractor's engagement leadership shall review quarterly, at a minimum, the effectiveness of the entire CIP approach to ensure appropriate identification, management, and implementation of service improvements in alignment with TennCare's objectives and approach for the CIP.

A.11.12.4. The Contractor shall be responsible for developing and implementing a CIP that aligns with Industry Standards and Policies (e.g., ITIL or Six Sigma) and is approved by TennCare.

A.11.12.5. The Contractor shall continuously identify and present improvement opportunities within each service function, process, and activity to maximize the service performance, value, and functionality to TennCare for feasibility reviews at a cadence determined by TennCare.

A.11.12.6. The Contractor shall manage a CIP backlog of improvement opportunities identified jointly by TennCare and the Contractor for all activities to maximize performance, value, and functionality.

A.11.12.7. The Contractor shall track in the CIP backlog all relevant data related to individual improvement opportunities from identification to post-implementation analysis information.

A.11.12.8. The Contractor shall present implementation options and supporting materials, including relevant documentation, demonstrations, results of quantitative analysis, or other information as requested by TennCare, for CIP backlog items or specific items requested by TennCare for review and potential approval.

A.11.12.9. The Contractor shall implement TennCare-approved service improvements as an output of the CIP through TennCare's change management process.

A.11.12.10. The Contractor shall develop reports and Dashboards, as specified by TennCare, to support the CIP and make them available for TennCare review. Reports and Dashboards, including the underlying KPIs, shall be reviewed by TennCare on a cadence approved by TennCare and modified by the Contractor in order to mature the CIP and produce the best results.

A.11.12.11. The Contractor shall incorporate defined processes to conduct service reviews of ITSM activities for CIP opportunities.

A.11.12.12. The Contractor shall identify opportunities related to the MSS Solution to improve the services across the enterprise and enhance service offerings to Tennessee citizens.

A.11.12.13. The Contractor shall incorporate into service management processes regularly performed process assessments, benchmarking, and auditing activities, at a minimum monthly for each ITSM process or a timeline defined by TennCare, to drive innovation and improvement.

A.11.12.14. The Contractor shall be responsible for suggesting initiatives to improve services and quality for TennCare operations relating to the MSS Solution at a cadence agreed upon by TennCare.

Docusign Envelope ID: 40B7BFA4-E1BB-4360-9C9C-6FA33E97F12A

A.11.12.15. The Contractor shall be responsible for tracking the progress of CIP initiatives through post-implementation to confirm expected Benefits have been realized and document lessons learned.

A.11.12.16. The Contractor shall provide feedback to the CIP service review and evaluation processes for future planning initiatives.

A.11.12.17. The Contractor shall review logs and trend reports on a regular interval approved by TennCare to identify suspicious or questionable activity for investigation and documentation as to their cause and remediation.

A.11.13. Technical Management

A.11.13.1. The Contractor shall be responsible for the technical management function of the MSS Solution, providing technical skills and capabilities in support of TennCare services, and management of the MSS. The Contractor shall define the roles of support teams, tools, processes, and procedures required to achieve acceptable service levels as defined by TennCare.

A.11.13.2. The Contractor shall be responsible for the desktop support process and the overall responsibility for all of the Contractor's desktop and laptop computer hardware, software, and peripherals.

A.11.13.3. The Contractor shall install the State's VPN client onto Contractor-owned laptop/desktop machines in order to access tools and instruments on the State's network. TennCare will not provide TennCare-owned laptops to the Contractor.

A.11.14. Service Strategy

A.11.14.1. The Contractor shall support the ongoing refinement of the TennCare Service Strategy through collaborative activities in alignment with TennCare priorities and goals.

A.11.14.2. The Contractor shall participate in technical and business planning sessions to establish security standards, architecture, and project initiatives.

A.11.14.3. The Contractor shall monitor patterns of MSS business activity and provide suggestions for performance optimization for TennCare approval.

A.11.14.4. The Contractor shall confirm and optimize performance and cost to ensure production services perform as expected from a business user perspective.

A.11.14.5. The Contractor shall support TennCare in identification and resolution of known performance issues related to IT services affecting Business Processes.

A.11.14.6. The Contractor shall support TennCare's Service Strategy strategic management activities related to IT services.

A.11.15. IT Service Continuity Management

A.11.15.1. The Contractor shall develop requirements and continuity plans for managing risks that could impact Services to ensure that the MSS Solution can always provide minimum agreed SLAs, in accordance with Deliverables as detailed in MSS TennCare Solution Implementation Lifecycle RACI and Deliverables including, but not limited to, the Business Continuity/Disaster Recovery Plan and Privacy Impact Assessment.

A.11.15.2. The Contractor shall ensure development, use, and updating of continuity plans at intervals determined by TennCare for MSS.

A.11.15.3. The Contractor shall ensure testing of components critical to recovery plans at a cadence defined by TennCare.

Docusign Envelope ID: 40B7BFA4-E1BB-4360-9C9C-6FA33E97F12A

A.11.16. Information Security Management

A.11.16.1. The Contractor shall adhere to all TennCare security requirements and standards.

A.11.16.2. The Contractor shall support production, updating, and improvement of security policies and controls.

A.11.16.3. The Contractor shall fully support TennCare in implementing approved security policies.

A.11.16.4. The Contractor shall be responsible for conducting assessments of information assets and risks, at a cadence approved by TennCare, and providing reporting to TennCare.

A.11.17. Performance Management

A.11.17.1. The Contractor shall monitor and analyze performance data to identify MSS Solution performance issues and improvement opportunities.

A.11.17.2. The Contractor shall analyze the performance data of the MSS Solution patterns, trends, and insights to enhance the performance of TennCare enterprise solutions.

A.11.17.3. The Contractor shall be responsible for investigating performance issues related to MSS Solution to resolution and providing relevant documentation to TennCare.

A.11.17.4. The Contractor shall support TennCare, in the design and implementation of a high-performance MSS Solution to achieve and exceed minimum acceptable service levels, as defined in Attachment B, Service Level Agreements and Liquidated Damages.

A.11.17.5. The Contractor shall be responsible for reviews of the service delivery framework, at a cadence approved by TennCare, for performance improvements to:

A.11.17.5.1. Ensure that Service Design activities incorporate performance improvement opportunities and outputs from the CIP process; and

A.11.17.5.2. Ensure that performance improvement opportunities drive service strategy development.

A.11.18. Knowledge Management

A.11.18.1. The Contractor shall be responsible for defining a MSS knowledge management strategy for TennCare approval and alignment of the MSS knowledge management processes to the TennCare Enterprise Knowledge Management Strategy.

A.11.19. Access Management

A.11.19.1. The Contractor shall support TennCare activities regarding coordination and support of access management activities.

A.11.19.2. The Contractor shall be responsible for management of the MSS Solution access verification and validation of access requisition activities.

A.11.19.3. The Contractor shall be responsible for monitoring, tracking, and controlling access to the MSS Solution.

A.11.19.4. The Contractor shall be responsible for de-provisioning access for users and the MSS Solution.

Docusign Envelope ID: 40B7BFA4-E1BB-4360-9C9C-6FA33E97F12A

A.11.20. Turnover

A.11.20.1. If applicable, the Contractor shall cooperate with TennCare in transitioning the MSS Solution and responsibilities of this Contract to TennCare, authorized contractor, and/or successor contractor upon termination, expiration, or Partial Takeover of this Contract. This shall include knowledge transfer, operating processes and procedures, all documents, and playbooks relevant to services provided to TennCare.

A.11.20.2. All documentation, service processes, data and methodologies developed for the services delivered to TennCare will become the property of TennCare in accordance with Contract Sections E.3 and E.10.

A.11.20.3. The Contractor shall develop a Turnover Plan for transitioning work from a prior vendor and to a successor vendor as required by TennCare.

A.11.20.4. The Contractor shall actively participate in Transition Planning & Management.

A.11.20.5. The Contractor shall deliver to TennCare, or its authorized representative, all Contract-related records and data in a format specified by TennCare, thirty (30) calendar days prior to Contract expiration or thirty (30) calendar days after TennCare's request.

A.11.20.6. The Contractor shall ensure that a Turnover Plan, as defined in Attachment A, Definitions is delivered and approved by TennCare. The Contractor shall also provide an updated version of the Turnover Plan at a minimum of one hundred eighty (180) calendar days prior to the Contract end date. The Turnover Plan shall include:

A.11.20.6.1. A timeline with milestones for the Turnover to include planning, execution, and implementation approval.

A.11.20.6.2. Description of maintenance process for Turnover documentation and Artifacts throughout the life of the Contract.

A.11.20.6.3. Any additional information requested by TennCare in a Control Memorandum.

A.11.20.7. The Contractor shall, always, act in good faith toward the State and/or Successor Contractor to facilitate as seamless a transition as possible. The State will use the Control Memorandum process (as described in Section A.12.6) to specify Turnover deliverables, services, and support required of the Contractor in aid of the transition process, including but not limited to::

A.11.20.7.1. Security profiles of the platform users and service accounts in a Microsoft Word document, Microsoft Excel spreadsheet format, or other format as approved by TennCare.

A.11.20.7.2. Turnover Deliverables that are considered TennCare customizations, archived and current data, and assets that are non-proprietary aspects of the COTS solution as requested by TennCare and in a format acceptable to TennCare.

A.11.20.8. Failure to fully and timely cooperate with the State's request or provide requested Turnover deliverables may result in liquidated damages as specified in this Contract or in the applicable Control Memorandum. The State shall not be liable to the Contractor for any costs and expenses relating to these deliverables or to the services provided by the Contractor during the transition period, other than as set forth in Contract Section C.

A.11.20.9. The Contractor shall provide post-Turnover support for up to one hundred twenty (120) calendar days, including Deliverables and associated activities specified in a Control Memorandum and agreed to by TennCare.

Docusign Envelope ID: 40B7BFA4-E1BB-4360-9C9C-6FA33E97F12A

A.11.20.10. The Contractor shall complete financial reconciliation of this Contract, including liquidated or financial consequences, if applicable.

A.12. Administrative Requirements

A.12.1. Staffing

A.12.1.1. General Staffing Requirements

A.12.1.1.1. The Contractor shall meet all TennCare and Federal and State regulations regarding required training to perform their duty.

A.12.1.1.1.1. The Contractor must complete security and privacy training and submit compliance reports to the TennCare Privacy Officer in accordance with TennCare Security policies, and standards located in Attachment C, Procurement Library or as otherwise requested during the term of the Contract and during any renewal period.

A.12.1.1.1.2. The Contractor must provide copies of all security and privacy training materials and training completion records upon request by TennCare.

A.12.1.1.2. All personnel shall be employees or subcontractors of the Contractor and fully qualified to perform the work required in this Contract. The Contractor shall provide experienced, qualified professionals to be engaged with TennCare. The Contractor shall provide personnel in sufficient quantity to meet all requirements of the Contract.

A.12.1.1.3. The Contractor shall maintain their Key Personnel latest contact details and provide to TennCare.

A.12.1.1.4. The Contractor shall provide diversified analysts across the Country and shall provide this information to TennCare upon request.

A.12.1.1.5. The Contractor's work shall occur 24x7x365, during which the Contractor must provide coverage of business areas as determined by TennCare.

A.12.1.1.6. Other than required approval of Key Personnel and subcontractors by TennCare as detailed in A.12.2.1.3., the Contractor shall have the responsibility for hiring and management of all Contractor staff and subcontractors. The Contractor shall be responsible for maintaining a level of staffing necessary to perform and carry out all Services required by this Contract, regardless of the level of staffing included in its proposal. After consultations with the Contractor, TennCare shall make the final decision as to the required staffing levels based upon current progress in meeting the goals of the SOC and anticipated future needs for the SOC. TennCare will use the CM process to indicate dates by which staffing increases or replacements must be made. Failure to meet the staffing deadlines in the CM may lead to the imposition of Liquidated Damages as specified in Attachment B, Service Level Agreements and Liquidated Damages.

A.12.1.1.7. The Contractor shall ensure that the roles that are established to support Operations and Maintenance and that are staffed shall be included in the measurement of Operations and Maintenance headcount for a given period, even though they may also be supporting enhancement activity for the same period.

A.12.1.1.8. TennCare shall have the discretion to approve or disapprove the Contractor's and any of its subcontractor's staff or to require the removal or reassignment of any of Contractor's or subcontractor's staff found unacceptable to TennCare for work under this Contract only.

Docusign Envelope ID: 40B7BFA4-E1BB-4360-9C9C-6FA33E97F12A

A.12.1.1.9. The Contractor shall keep track of resource costs, both personnel and technical, on a per project basis in order to satisfy TennCare and CMS reporting requirements for enhanced federal funding assistance. These resource costs shall be maintained by the Contractor and provided to TennCare, upon request, to support all projects. After consultation with the Contractor, TennCare will approve an invoice format that will meet the needs of TennCare and CMS. The Contractor shall submit an invoice as required by Section C.5 for approval once TennCare has issued Acceptance of the Deliverable.

A.12.1.1.10. The Contractor shall ensure that Contractor has sufficient, appropriately trained, and experienced staff to successfully operate both the business and technical functions of the SOC from contract execution through operations.

A.12.1.2. Subcontracted Staff

A.12.1.2.1. With regard to those subcontractors approved by TennCare in accordance with Section D.7, the Contractor shall provide TennCare with a fully executed, complete copy of each subcontract on or before the earlier of: (a) such subcontractor beginning work on this Contract or (b) within thirty (30) days of execution of the Contract. With regard to subcontractors approved by TennCare and engaged by Contractor after the Contract start date, the Contractor shall provide TennCare with a fully executed, complete copy of each subcontract on or before the earlier to occur of: (a) such subcontractor beginning work on this Contract or (b) within thirty (30) days of TennCare's approval of the subcontract.

A.12.1.2.2. The Contractor shall not substitute a subcontractor for a subcontractor previously approved by TennCare without the prior written approval of TennCare, as required by D.7.

A.12.2. Key Personnel

A.12.2.1. General Requirements

A.12.2.1.1. Section A.12.2.5. Table 2 – Key Personnel contains the required Key Personnel positions, corresponding roles and responsibilities, and minimum qualifications for each.

A.12.2.1.2. All Key Personnel shall be employees of the Contractor.

A.12.2.1.3. The Contractor shall obtain TennCare's prior written approval of all Key Personnel. The Contractor shall provide resumes for all Key Personnel to TennCare at least thirty (30) days prior to the expected employee's start date on this Contract. TennCare reserves the right to conduct in-person interviews with Key Personnel prior to the Key Personnel's start date on this Contract. The Contractor may utilize the same personnel for more than one (1) Key Personnel position in different Gate Reviews with prior written approval from TennCare. The Contractor shall not make any changes to the proposed positions, staff, and responsibilities of Key Personnel without TennCare's prior written approval.

A.12.2.1.4. If the Contractor deems additional Key Personnel position(s) necessary beyond the positions listed in Table 2 – Key Personnel below, the Contractor shall identify these positions and provide a complete description of how these positions support the fulfillment of the Contract. TennCare, at its sole discretion, shall determine if additional Key Personnel position(s) are necessary for this Contract. All Key Personnel proposed during the procurement of this Contract shall be part of the Key Personnel team for TennCare pursuant to Contract Section A.12.2.1.9.5. All Key Personnel must be formally committed to join the project by the

Docusign Envelope ID: 40B7BFA4-E1BB-4360-9C9C-6FA33E97F12A

Contract Effective Date. All requirements for TennCare pre-approval of Key Personnel, as detailed in A.12.2.1.3, shall apply to Key Personnel additions.

A.12.2.1.5. The Contractor shall not employ or use a subcontractor without the written approval of TennCare.

A.12.2.1.6. References for Key Personnel shall meet the following requirements:

A.12.2.1.6.1. A minimum of three (3) professional references outside the employee's current employer who can provide information about the Key Personnel's work on relevant past assignments;

A.12.2.1.6.2. The reference's full name, mailing address, telephone number, and e-mail address; and

A.12.2.1.6.3. For any client contact listed as a reference, include the agency's or company's full name with the current telephone number and e-mail address of the client's responsible project administrator or service official who is directly familiar with the Key Personnel's performance.

A.12.2.1.7. Key Personnel resumes shall include the following information:

A.12.2.1.7.1. Employment history for all relevant and related experience;

A.12.2.1.7.2. Names of employers for the past five (5) years, including specific dates;

A.12.2.1.7.3. All educational institutions attended, and degrees obtained; and

A.12.2.1.7.4. All professional certifications and affiliations.

A.12.2.1.8. The Contractor shall provide guidance on the necessary steps to make staffing assignment changes. The Contractor shall also define procedures for Key Personnel transitions for TennCare approval.

A.12.2.1.9. TennCare retains the right to approve or disapprove proposed Key Personnel staffing and reserves the right to require the Contractor to replace specified staff. The Contractor shall substitute, with TennCare's prior approval, any employee so replaced with an employee of equal or better qualifications. The Contractor shall provide an interim employee within five (5) Business Days of any Key Personnel vacancy regardless of the reason for the vacancy. The Contractor shall propose a substitute employee within thirty (30) days, and the Contractor shall ensure that the substitute employee begins work for the Contractor within forty-five (45) days. If the Contractor does not provide Key Personnel in compliance with each of the three (3) stated timeframes, the Contractor will be assessed Liquidated Damages in accordance with Attachment B, Service Level Agreements and Liquidated Damages. In the event it becomes necessary to replace Key Personnel during the term of this Contract, the Contractor shall:

A.12.2.1.9.1. Provide TennCare's Chief Information Security Officer or designee with written notification of such replacement, providing, when possible, for a two (2) week period for knowledge transfer from the Key Personnel to the replacement personnel. This knowledge transfer shall be provided at no charge to TennCare;

A.12.2.1.9.2. Provide TennCare's Chief Information Security Officer or designee with documentation describing the circumstances of the need for the replacement;

Docusign Envelope ID: 40B7BFA4-E1BB-4360-9C9C-6FA33E97F12A

A.12.2.1.9.3. Provide documentation of experience for the proposed replacement personnel;

A.12.2.1.9.4. Obtain prior written approval from TennCare's Chief Information Security Officer or designee; and

A.12.2.1.9.5. During the first twelve (12) months of the Contract performance period, no substitutions of Key Personnel shall be permitted unless such substitutions are necessitated by an individual's sudden illness, death, or resignation, or otherwise approved by TennCare's Chief Information Security Officer or designee, or requested by TennCare. In any of these events, the Contractor shall follow the steps outlined in this Section. Failure to meet the prior notice and approval requirements herein may result in the imposition of Liquidated Damages as contained in Attachment B, Service Level Agreements and Liquidated Damages.

A.12.2.2. Staffing Needs, Planning, and Monitoring Processes

A.12.2.2.1. The Contractor shall provide an overview report of the preliminary and ongoing staff planning and monitoring Processes at a frequency determined by TennCare. The report shall specifically identify activities for planning for future needs and monitoring of the project assignments, contract timelines, the nature of existing and anticipated vacancies, length of time a position has been vacant, status of hiring, and associated decisions for release or renewal of personnel.

A.12.2.3. Turnover Staffing

A.12.2.3.1. The Contractor shall provide a full-time Turnover Manager one-hundred eighty (180) calendar days prior to the end of the Contract as a designated point person to interact with TennCare and a successor contractor, if applicable, until Contract Term is completed.

A.12.2.3.2. The Contractor shall provide and retain sufficient Key Personnel resources during Turnover, inclusive of technical staff (e.g. systems analysts, technicians) and non-technical staff (e.g. clerical staff, business analysts) resources to complete the Services and meet the requirements specified in the Contract.

A.12.2.3.3. The Contractor shall include staffing for operations during Turnover in the Turnover Plan.

A.12.2.4. Onboarding / Off-Boarding

A.12.2.4.1. The Contractor shall appoint a Contractor liaison who is responsible for completing an off-boarding request in the ITSM tool within twenty-four (24) hours of a resource departure.

A.12.2.4.2. In the event of a Key Personnel departure during the term of this Contract, the Contractor shall provide prior notification, with appropriate forms to TennCare's Access Management team and appropriate TennCare management staff in advance of termination, if known, or immediately after the resource submits their resignation.

A.12.2.4.3. The Contractor shall meet background check requirements as defined by TennCare prior to accessing TennCare data. The Contractor shall maintain a list of employees authorized with access and will provide the list upon TennCare's request.

Docusign Envelope ID: 40B7BFA4-E1BB-4360-9C9C-6FA33E97F12A

A.12.2.5. Key Personnel Table.

TABLE 2: KEY PERSONNEL TABLE

Key Positions	Description	Minimum Qualification	Requirements
Project Manager	The Project Manager, in collaboration with the TennCare Project Manager, is responsible for managing daily operations, realign staff, and ensure delivery and timeliness of customer satisfaction. Shall perform the tasks below at a minimum: - Incident response coordination - Provide metrics data to TennCare Management - Provide leadership and direction to information technology (IT) personnel by ensuring that cybersecurity awareness, basics, literacy, and training are provided to analysts - Ensure all security operations activities are properly documented and updated as necessary	- Shall possess a minimum of five (5) years of experience in leading a Managed SOC. - Shall possess strong technical expertise, strong leadership qualities and a deep understanding of cybersecurity best practices.	- Shall not serve in any other position - Shall be available as needed
L2 SOC Analyst	L2 SOC Analyst will serve as a technical escalation resource for L1 SOC Analysts and provide mentoring for skill development. L2 SOC analyst perform threat analysis and investigations, provide remediation recommendations to TennCare, and support client response actions. Shall perform the tasks below at a minimum: - 24x7x365 Security event monitoring - Incident analysis and investigation - Threat Intel Correlation - Provide containment and recovery guidance - Support Client response actions - Update SOPs or Playbooks - Support Onsite breach investigations - Support digital forensics - Defining logic for SOAR playbooks	- Shall possess a minimum of five (5) years of experience in working in a Managed SOC. - Shall possess a strong technical expertise in threat analysis.	- Shall not serve in any other position. - Shall be available for 24x7x365 rotation - Shall be available as needed

Docusign Envelope ID: 40B7BFA4-E1BB-4360-9C9C-6FA33E97F12A

Key Positions	Description	Minimum Qualification	Requirements
	- Reporting - Maintain Threat Intelligence feeds within SIEM		
L1 SOC Analyst	As a Level 1 SOC Analyst, the analyst is focused on real-time SIEM monitoring and is responsible for triaging alerts, gathering additional information, running ad-hoc and scheduled reporting, reviewing reports and dashboards, and escalate to L2 SOC Analysts as needed. Shall perform the tasks below at a minimum: - 24x7x365 Security event monitoring - Event triage - Information gathering - Incident analysis and support investigation - Support Client response actions - Reporting	- Shall possess a minimum of two (2) years of experience in working in a Managed SOC. - Shall possess a strong technical expertise in threat analysis.	- Shall not serve in any other position. - Shall be available for 24x7x365 rotation - Shall be available as needed
Threat Analyst	As a threat analyst, the analyst is focused on gathering, analyzing and interpreting Threat Intelligence data to identify potential risks and develop strategies to mitigate these risks. Shall perform the tasks below at a minimum: - Monitor and analyze emerging cyber threats - Collect and assess data to identify potential risks to TennCare's infrastructure, systems and data - Develop and maintain threat profiles, indicators of compromise and patterns of malicious activities to enhance detection and response capabilities - Participate in Incident Response Activities - Reporting	- Shall possess a minimum of three (3) years of experience in working in a Managed SOC. - Shall possess a strong technical expertise in threat analysis. - Strong experience in Threat Intelligence platforms. - At least one year experience with Splunk.	- Shall not serve in any other position. - Shall be available as needed
SIEM Engineer	The SIEM Engineer shall act as a Subject Matter Expert for SIEM and able to develop and deliver new and enhanced SIEM Content items. Perform log source or application onboarding	- Shall possess a minimum of five (5) years of experience in SIEM engineering - Shall possess a strong Content Management and	- Shall not serve in any other position. - Shall be available as needed

Docusign Envelope ID: 40B7BFA4-E1BB-4360-9C9C-6FA33E97F12A

Key Positions	Description	Minimum Qualification	Requirements
	Shall perform the tasks below at a minimum: - Implement and manage SIEM Content Development Pipeline - SIEM Content development and tuning - SIEM Log source/Application onboarding - Conduct onboarding prioritization in conjunction with TennCare - SIEM health monitoring and application management - Reporting	Logsource/application onboarding experience	

Docusign Envelope ID: 40B7BFA4-E1BB-4360-9C9C-6FA33E97F12A

A.12.3. Facility

A.12.3.1. The Contractor shall leverage TennCare's video conferencing and collaboration licenses and tools (e.g., WebEx, Microsoft Teams, Cisco TelePresence MX300 G2, and MX200 G2), where possible.

A.12.3.2. The Contract shall not permit the Contractor's employees, agents, representatives, or subcontractors to share, store, access, use, transport, or disclose TennCare data in any form via any medium, including with any third parties, beyond the boundaries and jurisdiction of the United States of America without the express written authorization from TennCare.

A.12.3.3. The Contractor shall not permit the Contractor's employees, agents, representatives, or sub-contractors to perform any activities required by this Contract outside of the boundaries and jurisdiction of the United States, or to use any systems infrastructure, components, or resources located outside of the United States to support these activities, without obtaining express written authorization from TennCare.

A.12.3.4. The Contractor shall ensure that all facilities supporting this Contract are protected against threats, during working and non-working hours, with an appropriate surveillance alarm/system extended to a manned monitoring system extended to a manned monitoring center, in accordance MARS-E (current version) and IRS Pub 1075 (current version).

A.12.3.5. The Contractor shall deliver equivalent Service performance via enhanced use of teleconferencing, collaboration, and Workflow tools to fulfill all requirements of this Contract at TennCare's request.

A.12.4. Warranty

A.12.4.1. General Requirements

A.12.4.1.1. The Contractor represents and warrants that the term of the "Warranty Period" for the MSS shall be the greater of the Term of this Contract or any other warranty generally offered by Contractor, its suppliers, or manufacturers to customers of its good or services. The goods or services provided under this Contract shall conform to the terms and conditions of this Contract throughout the Warranty Period. Any nonconformance of the goods or services to the terms and conditions of this Contract shall constitute a "Defect" and shall be considered "Defective." If Contractor receives notice of a Defect during the Warranty Period, then Contractor shall correct the Defect, at no additional charge. Incidents and Problems identified during the Warranty Period may be considered Defects as determined by TennCare.

A.12.4.1.2. The Contractor represents and warrants that TennCare is authorized to possess and use all equipment, materials, software, and Deliverables provided under this Contract.

A.12.4.1.3. The Contractor represents and warrants that all goods or services provided under this Contract shall be provided in a timely and professional manner, by qualified and skilled individuals, and in conformity with standards generally accepted in Contractor's industry.

A.12.4.1.4. If Contractor fails to provide the goods or services as warranted, then Contractor will re-provide the goods or services at no additional charge. If Contractor is unable or unwilling to re-provide the goods or services as warranted, then TennCare shall be entitled to recover the fees paid to Contractor for the Defective goods or services. Any exercise of

Docusign Envelope ID: 40B7BFA4-E1BB-4360-9C9C-6FA33E97F12A

TennCare's rights under this Section shall not prejudice TennCare's rights to seek any other remedies available under this Contract or applicable law.

A.12.4.1.5. In the event that a subsequent release creates or identifies Defects, the Warranty Period of the created or identified Defect will be covered by the Warranty of that subsequent release.

A.12.4.2. Documentation and Resolution of Warranty Defects

A.12.4.2.1. The Contractor shall classify Warranty Defects as severity level 1, 2, 3, and 4, as described in Attachment B, Service Level Agreements and Liquidated Damages, and track Warranty Defects.

A.12.4.2.2. The identification of critical and high Defects during the Warranty Period shall extend the Warranty Period for Solution for six (6) months after the time of the resolution of critical or high Defects.

A.12.4.2.3. The Contractor shall be responsible to resolve all critical and high Warranty Defects within the periods described in Attachment B, Service Level Agreements and Liquidated Damages, or, if necessary, provide TennCare with a mutually acceptable timeframe and written work-around, downstream impacts, and plan for resolution, all without additional cost to TennCare.

A.12.4.2.4. The Contractor shall resolve all medium and low Defects within the periods described in Attachment B, Service Level Agreements and Liquidated Damages.

A.12.4.2.5. The Contractor shall be subject to corresponding Liquidated Damages, listed in Attachment B, Service Level Agreements and Liquidated Damages, for all identified Warranty Defects that are not resolved within the associated resolution timeframes.

A.12.4.3. Inspection and Acceptance. The State shall have the right to inspect all goods or services provided by Contractor under this Contract. If, upon inspection, the State determines that the goods or services are Defective, the State shall notify Contractor, and Contractor shall re-deliver the goods or provide the services at no additional cost to the State. If after a period of thirty (30) days within discovery by the State of nonconforming goods or services and the State does not provide a notice of any Defects, the goods or services shall be deemed to have been accepted by the State.

A.12.5. Change Order- Special Projects & Enhancements

A.12.5.1. General Requirements

A.12.5.1.1. Special Projects or Enhancements are additional projects that TennCare may, at its sole discretion, initiate and assign to the Contractor during the Contract for the performance of services, fulfillment of additional requirements, or creation of Deliverables or Services that are within the Scope of this Contract but were inadvertently unspecified.

A.12.5.1.2. Changes Orders for each Special Project or Enhancement shall be implemented by a Control Memorandum as described in this Section A.12.5 and Section A.12.6.

A.12.5.2. Support Change Requests

A.12.5.2.1. The Contractor shall review Business Services Definitions issued by CMS and provide TennCare with a solution impact analysis on requirements

Docusign Envelope ID: 40B7BFA4-E1BB-4360-9C9C-6FA33E97F12A

and interfaces within seven (7) calendar days of receipt of a Change Request.

A.12.5.2.2. The Contractor shall perform impact analysis on Change Requests to identify impacts across Business Processes and business rules.

A.12.5.2.3. The Contractor shall perform risk analysis on Change Requests to identify risks and potential mitigations associated with development and deployment of the change.

A.12.5.2.4. The Contractor shall perform alternatives analysis for Change Requests to support the Medicaid Modernization Project Steering Committee (Project Steering Committee) with relevant information concerning alternative approaches to addressing the business need underlying the request.

A.12.5.2.5. The Contractor shall perform cost analysis for Change Requests as part of the Change Order process described in Section A.12.5. All Change Requests shall indicate implementation and full lifecycle costs for the proposed change.

A.12.5.2.6. The Contractor shall work with TennCare management to identify the impact of human resource costs as well as cross-project impacts associated with fulfilling the Change Request.

A.12.5.2.7. The Contractor shall provide analysis to support timing decisions for deployment of Change Requests in compliance with TennCare's release management process.

A.12.5.3. Change Order Creation

A.12.5.3.1. After receipt of a written request for the performance of Services, the Contractor shall respond to TennCare, within ten (10) Business Days, with a written proposal in the form of a draft Control Memorandum for completing the Services to fulfill TennCare's request for Services in a cost-effective manner. Contractor's proposal shall specify:

A.12.5.3.1.1. The effect, if any, of implementing the requested change(s) on all other services required under this Contract. The Contractor shall provide TennCare, in writing, a listing of all anticipated or perceived impacts to the Contractor's Solution and any integrating Solution, to include the written impact specifications of the corresponding Contractor;

A.12.5.3.1.2. A description of the units of service needed to complete the change(s);

A.12.5.3.1.3. The specific effort involved in completing the change(s);

A.12.5.3.1.4. The expected schedule for completing the change(s);

A.12.5.3.1.5. The maximum number of person hours required for the change(s); and

A.12.5.3.1.6. A fixed price for all change(s) under the Change Order based on the Contractor's rate card as detailed in this Contract. The maximum cost for the Services shall in no instance exceed the product of the person hours required multiplied by the appropriate Payment rate proposed for such work.

A.12.5.3.2. The Contractor shall not perform any Services under the Change Order until TennCare has approved the Change Order proposal through a

Docusign Envelope ID: 40B7BFA4-E1BB-4360-9C9C-6FA33E97F12A

Control Memorandum (CM) containing a Control Directive that is signed by both TennCare and the Contractor. If approved, the CM and Change Order shall constitute a binding agreement between the Parties pertaining to the specified change(s) and shall, under this provision, be incorporated into this Contract by reference. All terms of this Contract, including, but not limited to, Warranty, Service Level Agreements, and Liquidated Damages shall apply to Services provided under Change Orders.

A.12.5.3.3. Subsequent to creation and authorization of a Change Order through a CM signed by both Parties, the Contractor shall complete the required Services. TennCare shall be the sole judge of the acceptable completion of Services and, upon such determination, TennCare shall provide the Contractor written approval of satisfactory completion of the CO services. Contractor shall submit such written approval as part of the invoicing documentation when Contractor requests payment for such Services.

A.12.5.3.4. TennCare will remunerate the Contractor only for work TennCare has (1) requested through a CO authorized by a CM and Control Directive signed by both Parties and (2) which TennCare has deemed acceptable. All acceptable work performed pursuant to an approved Change Order shall be remunerated in accordance with Contract Section C.3. Provided that, TennCare shall be liable to the Contractor only for the actual cost of the goods or Services completed, not to exceed the maximum cost for the change detailed in the Change Order. In no instance shall TennCare be liable to the Contractor for any amount exceeding the maximum cost specified by the Change Order. Upon TennCare approval of the work, the Contractor shall invoice TennCare in accordance with Section C.3.

A.12.6. Control Memorandum Process

A.12.6.1. The Control Memorandum (CM) process shall be utilized by TennCare to clarify Contract requirements, issue instruction to the Contractor, document action required of the Contractor, or request information from the Contractor. In addition, the CM process shall be used by TennCare to impose assessments of damages, either actual or liquidated. This process will be used to address issues or matters that do not require a contract amendment. Each CM must be in writing and indicate the date on which it was issued. CMs may provide relevant history, background, and other pertinent information regarding the issue(s) being addressed in the CM. Each CM will establish a deadline or timeframe for the Contractor's reply or other action. All CMs submitted to the Contractor must be signed and approved by TennCare's Project Director (or his/her designee). When the CM pertains to damages, either actual or liquidated, TennCare may issue consecutive CMs, as may be necessary or appropriate.

A.12.6.2. A CM may include one (1) or more of the five (5) components of the CM process described below:

A.12.6.2.1. On Request Report – a request directing the Contractor to provide information by the time and date set out in the CM;

A.12.6.2.2. Control Directive (CD) – instructions that require the Contractor to complete, within a designated timeframe, one (1) or more Deliverables or to perform any other request from TennCare that is within the scope of the Contract. A CD may also provide clarification of certain Contract terms. Once a CM/CD has been issued, it shall be considered to be incorporated into this Contract;

A.12.6.2.3. Notice of Potential Damages (Actual or Liquidated) (NPD) – notification to the Contractor that TennCare has determined that a

Docusign Envelope ID: 40B7BFA4-E1BB-4360-9C9C-6FA33E97F12A

potential Contract performance or compliance failure exists and that TennCare is contemplating assessing damages, actual and/or liquidated. The NPD shall identify the Contract provision(s) on which TennCare's determination rests;

A.12.6.2.4. Notice of Calculation of Potential Damages (Actual or Liquidated) (NCPD) – notification to the Contractor that provides a calculation of the amount of potential damages, actual and/or liquidated, that TennCare is contemplating assessing against the Contractor. NPDs and NPCDs may be issued consecutively or simultaneously; or

A.12.6.2.5. Notice of Intent to Assess Damages (Actual or Liquidated) (NIAD) – notification to the Contractor that TennCare is assessing damages and specifying whether the damages are actual damages or Liquidated Damages and setting out the performance or compliance issue underlying each intended damage assessment. The NIAD shall identify the NPD and NCPD upon which it is based. The NIAD shall specify the total amount and type of damages, whether actual or liquidated, TennCare intends to assess. Following the issuance of an NIAD, TennCare may elect to withhold damages from Payments due to Contractor. TennCare may not issue a NIAD without first issuing an NPD and a NPCD. TennCare may not obtain both Liquidated Damages and Actual Damages for the same occurrence of a Contract performance failure.

A.12.6.3. Failure to comply with CM. The Contractor shall fully comply with all CMs, compliance to be determined in TennCare's sole discretion. Failure to do so may result in TennCare pursuing recovery of damages, as defined in Contract Section E.16., including Liquidated Damages as listed in Attachment B, Service Level Agreements and Liquidated Damages, a corrective action plan approved by TennCare, and/or termination of the Contract.

A.12.6.4. Appeal of Damages by Contractor. Contractor may appeal either the basis for NPD or calculation of NCPD potential damages, either actual or liquidated. To do so, the Contractor shall submit to the TennCare's Project Director (or his/her designee) a written response to the NPD and/or NCPD within ten (10) Business Days of receipt of a CM which includes an NPD or a NCPD. TennCare's Project Director (or his/her designee) shall review the appeal and provide notice of his/her determination to the Contractor through a CM. If the Contractor disagrees with TennCare's Project Director's (or his/her designee) initial appeal determination or TennCare's Project Director (or his/her designee) is unable to resolve the appeal, the Contractor may submit a written request to TennCare's Project Director (or his/her designee) that the matter be escalated to senior management of TennCare. Contractor shall submit such a request for escalation within ten (10) Business Days of its receipt of the initial appeal determination from TennCare's Project Director (or his/her designee) or of notification by TennCare's Project Director that he/she is unable to resolve the appeal. TennCare's senior management shall provide written notice of its final determination to the Contractor within (10) days of the receipt of the appeal from the Contractor. Upon appeal or escalation, TennCare shall not increase the amount of the potential damages.

A.12.6.5. Implement Corrective Action Plan. At TennCare's discretion, TennCare may, through a CM and Control Directive, issue a notice to the Contractor of its intention to impose a Corrective Action Plan (CAP) with the CM, accompanied by a request that the Contractor develop and propose an appropriate CAP within ten (10) days for review and approval by TennCare. TennCare shall determine the severity of the error using the Incident definitions as set forth in Attachment B, Service Level Agreements and Liquidated Damages.

Docusign Envelope ID: 40B7BFA4-E1BB-4360-9C9C-6FA33E97F12A

A.12.6.5.1. TennCare may, in its sole discretion, assess Liquidated Damages as set forth in the Liquidated Damages table located in Attachment B, Service Level Agreements and Liquidated Damages. Each CAP shall, at a minimum, contain the following information:

A.12.6.5.1.1. Written documentation that includes acknowledgment of receipt of TennCare notice;

A.12.6.5.1.2. Number of impacted Members and cases and such other information as TennCare may request;

A.12.6.5.1.3. A description of how the Contractor has addressed or will address the immediate Problem;

A.12.6.5.1.4. An analysis of the root cause of the Problem; and

A.12.6.5.1.5. A description of how the Contractor shall resolve the Problem (or has resolved the Problem) and shall prevent the Problem from recurring.

A.12.6.5.2. Upon Acceptance of the CAP by TennCare, the Contractor shall be responsible for executing the CAP, and the CAP shall be incorporated by reference as part of this Contract. TennCare may request changes and/or additions to an approved CAP as deemed necessary to correct or resolve the Problems that led to requesting a CAP. The Contractor shall continue to comply with an approved CAP until TennCare notifies the Contractor, in writing, that all Problems outlined in the CAP have been satisfactorily resolved.

A.12.6.5.3. The Contractor shall be responsible for ensuring that all of its subcontractors or service providers comply with all approved CAPs.

A.13. Table of Deliverables

A.13.1. The Contractor shall refer to the MSS TennCare Solution Implementation Lifecycle RACI and Deliverables for the minimum requirements of the Contractor Deliverables during the Implementation of the MSS and Operational activities.

A.13.2. The Contractor shall complete the Deliverables identified throughout the lifecycle phases of the TennCare Solution Implementation Lifecycle and MSS TennCare Solution Implementation Lifecycle RACI and Deliverables, as indicated in A.11. above. The MSS TennCare Solution Implementation Lifecycle Standard Document is organized into Phases and Gates with associated Deliverables that must be completed by Contractor and approved by TennCare. All Deliverables completed by Contractor and approved by TennCare shall be incorporated into this Contract. The MSS TennCare Solution Implementation Lifecycle RACI and Deliverables Table of Deliverables is included below as Table 3: Table of Deliverables for reference purposes only.

A.13.3. The Contractor shall ensure Deliverables also comply with the corresponding TennCare Standards Documentation, located in Attachment C, Procurement Library, where applicable.

Docusign Envelope ID: 40B7BFA4-E1BB-4360-9C9C-6FA33E97F12A

TABLE 3: TABLE OF DELIVERABLES

SILC Phase	Timing of Delivery	Deliverable	Deliverable Definition	Acceptance Criteria	Deliverable Classification
Concept Planning Requirements Review	Pre-Go Live	1. Project Management Plan	Baseline for project. High level PMP is initially approved during Concept phase and updated and approved once the MSS Vendor is on-boarded during Planning. It is updated as needed during Requirements Review. Contains: 1. Scope 2. Schedule 3. Cost 4. Quality 5. Staffing/resource management (includes Vendor Organization Charts when updated after Vendor On-Boarding), and hardware and software requirements 6. Stakeholder register 7. Communications 8. Status reports 9. Processes and standards to manage risks, issues, assumptions, action items, and constraints 10. Capacity planning 11. Once MSS Vendor is on-boarded, determine Bill of Materials, including key acquisition-related activities and items (e.g., costs for hardware, software, and service acquisitions)	Validation that: 1. The submitted Project Management Plan and all sub-plans listed below address all components of each of the TennCare Project Management Plan and sub-plan templates in alignment with PMBOK standards: a. Communication Management Plan b. Decision Management Plan c. Document Management Plan d. Human Resource Management Plan e. Quality Management Plan f. Risk Management Plan g. Issue Management Plan h. Schedule Management Plan i. Scope Management Plan	Type B
Concept Planning Requirements Review Development	Pre-Go Live	2. Implementation Schedule	The Implementation Schedule will be continually updated throughout project lifecycle. High level plan is initially approved during Concept phase, updated and approved again once the MSS Vendor is on-boarded during Planning. It is updated as needed during Requirements Review, and then once more before implementation go-live with the Implementation Plan.	Validation that the Implementation Plan: 1. Aligns with all Schedule Management Standards described in the TennCare Project Management Plan Standard 2. Is developed in Microsoft Project 3. Validates planning and readiness of all parties, including trading partners, impacted by the interface(s).	Type A
Planning	Pre-Go Live	3. Implementation Advanced Planning Document	APD/APD-U to describe the programmatic value, aligned to state priorities, that a state plans to achieve with their project. The APD/APD-U should include measurable outcomes and metrics that align with the desired Medicaid program goal(s). Contains: 1. Funding approval for the project 2. Requirements analysis 3. Feasibility study	1. Validation by TennCare Accounting and Budget departments on the financial information 2. Validation from TennCare IS on the financial information 3. Validation from	Type C

Docusign Envelope ID: 40B7BFA4-E1BB-4360-9C9C-6FA33E97F12A

SILC Phase	Timing of Delivery	Deliverable	Deliverable Definition	Acceptance Criteria	Deliverable Classification
			4. Alternatives analysis 5. Cost allocation plan 6. Proposed budget	TennCare Strategic Funding and Compliance Officer 4. Approval from TennCare Deputy Commissioner	
Planning	Pre-Go Live	4. Requirements Management Plan	Contains approach and methodology that the Solution Vendor will follow for managing requirements throughout the entire project.	Validation that: 1. The Requirements Management Plan is in alignment with TennCare Standards.	Type C
Requirements Review	Pre-Go Live	5. Contract Requirements Inventory,	The CRI contains the initial solution requirements and updated data requirements as published in the RFP for a Solution Vendor. It is updated throughout the lifecycle of the project.	Validation that: 1. The requirements in the CRI continue to align to TennCare's target state enterprise architecture and requirements as published in the RFP for a Solution Vendor. 2. The requirements meet the TennCare Data Policies and Standards. 3. Once the Solution Vendor is on-boarded, requirements are elaborated to a level of detail that is testable, with defined acceptance criteria. 4. The CRI approved at the Requirements Review Gate has the set of project level solution requirements traced to the complete set of original contract requirements, and traced to any CMS compliance criteria that are required for certification activities; with any exceptions annotated and approved. CRI: Traceability created, reports produced, updated continuously, reports generated as needed. *MORE:	Type C
Requirements Review	Pre-Go Live	6. Conceptual Data Model and Dictionary	The Conceptual Data Model and Dictionary defines the information types or subject areas that are required to support the business capabilities that are in scope of a transformation effort as described in the Concept of Operations and the contract	Validation that: 1. The Conceptual Data Model and Dictionary	Type C

Docusign Envelope ID: 40B7BFA4-E1BB-4360-9C9C-6FA33E97F12A

SILC Phase	Timing of Delivery	Deliverable	Deliverable Definition	Acceptance Criteria	Deliverable Classification
			requirements. The Conceptual Data Model and Dictionary are initially created as part of the Concept of Operations document during the Concept Phase, and updated at the start of the Requirements Review Phase as part of reviewing data requirements.	meets the standards prescribed in the TennCare Data Policies and Standards 2. The TennCare Enterprise Architecture Modeling Standard 3. The TennCare Enterprise Architecture Framework	
Requirements Review Design	Pre-Go Live	7. Logical Data Model and Dictionary	Define logical data models and dictionary that illustrate data concepts, entities, structures, and relationships to support the scope of the transformation effort. The logical data model does not prescribe physical data structures, but illustrates data requirements at a lower level of detail that the conceptual model. The logical model describes how data is related to itself, and business rules that must be enforced as a result of data requirements.	Acceptance Criteria	Type C
Requirements Review	Pre-Go Live	8. Risk Register / Exception Plan	List of project risks and mitigation plans for each. Completed by the Solution Vendor during on-boarding.	Validation that: 1. The project risks as outlined by the Solution Vendor are complete and accurate.	Type A
Design	Pre-Go Live	9. Test Management Plan	Contains the testing strategy for different types of testing, including unit testing, functional testing, regression testing, integration testing, user acceptance testing, performance testing, manual and automated and/or scripted testing, disaster recovery and end-to-end integration testing. Contains: 1. Testing schedule 2. Testing personnel 3. Training 4. Testing meetings 5. TennCare involvement 6. Collaboration with other vendors 7. Test cases, scripts and scenarios 8. Test data 9. Test environments 10. Tools 11. Test tracking and results 12. Defect management 13. Re-testing and regression testing 14. Test reporting and metrics	1. Validation that the deliverable includes acceptable plans and specifications, according to the Test Management Standard and the deliverable definition.	Type C
Design Implementation	Pre-Go Live	10. Technical Design Document	Contains the detailed specifications that will communicate the technical details required to develop the solution. It contains: 1. Technical architecture 2. Static code analysis (if applicable) 3. Code quality analysis (if applicable) 4. Enterprise system diagrams, including all components, identifying all logic flow, data flow, systems functions, and their associated data storage 5. A bi-directional traceability to requirements and test plan 6. Operational data design including how data should be created and maintained including Data Corrections, Data Retirement, Purge, Archive, and Retention -	Validation that: 1. The solution requirements show clear linkages to design components and are supported by defined acceptance test criteria 2. The design has demonstrated compliance with State and Federal	Type C

Docusign Envelope ID: 40B7BFA4-E1BB-4360-9C9C-6FA33E97F12A

SILC Phase	Timing of Delivery	Deliverable	Deliverable Definition	Acceptance Criteria	Deliverable Classification
			including defining secure disposal and complete removal of data from all storage media 7. Design of how Metadata including Business Metadata, Data Quality Metadata, Technical Metadata, Operational Metadata, should be defined, documented, monitored, tracked and reported. Technical metadata should include Data Transformation and Data Lineage from system of record to identified field 8. Data ownership and accountability with assigned responsibilities defined, documented, and communicated as defined by the TennCare Data Policies and Standards 9. Design of how data will be transmitted and received by TennCare modules and repositories - specifying data flow information. 10. Design of data quality controls and monitors to meet the specified data quality requirements. 11. Design of data history capture and audit processes and data structures to meet requirements. 12. Completed data classification as defined by the TennCare Data Policies and Standards 13. All policies and procedures for Data acquisition and capture, Data backup and recovery, Data management and maintenance, and Data retention and secure destruction as defined by the TennCare Data Policies and Standards 14. All relevant External data Policies and Standards as defined by the TennCare Data Policies and Standards May contain the Solution Architecture Model as defined in the EA Modeling Standard. Aligned to the TennCare Application Landscape and Inventory. See also the models in the Functional Design Document and the Infrastructure Plan.	accessibility requirements including Section 508 standards 3. Any identified design gaps have been documented and addressed as managed in the Risk Register / Exception Plan 4. The design supports and aligns with the State's solution release strategy 5. Completed assessment of all security controls related to requirements 6. The design addresses data conversion issues at the appropriate level	
Design	Pre-Go Live	11. Interface Control Design Document	A comprehensive report of a system interface, including but not limited to, types of transactions and data requirements for Interfaces covered in External Interfaces Agreements (EIAs). The Interface Control Design Document describes flow of data between systems. It describes the concept of operations, defines the governance of the data exchange, and identifies the communication paths of the expected data flow. An Interface Control Design Document is required for every interface. The design of how the data will be converted from existing data sources to the new structure includes the data quality/transformation rules that will be applied. It will document how data will be transmitted and received by TennCare modules and repositories as defined by the TennCare Data Policies and Standards. Aligned with the TennCare Interface Landscape and Inventory. The Integration Plan outlines and describes the general integration strategy, approaches, and standards established for the project. These guidelines are to then be applied in developing the individual Interface Control Documents (ICDs) which define each individual interface that is to be implemented and/or managed as part of a module implementation. Use of a clear XML Schema Definition (XSD) to capture data type, cardinality, and conditionality for all elements within Web Services. Describes a Web Service (WS) connectivity strategy for lower environments should be established and documented. If real-time connectivity isn't available, consider using a mock service. Establishes alerts to trigger in the event of a loss of connectivity with any inbound/outbound applications. Describes integration service contracts (e.g. API documentation) – including end points information.	Validation that the Interface Control Design Document defines: 1. The interface scope 2. The interface requirements 3. The interface performance requirements 4. The message formats or file layouts 5. The field/element level definitions for the data packets 6. The communication protocols for the interface 7. The security requirements for the interface	Type C

Docusign Envelope ID: 40B7BFA4-E1BB-4360-9C9C-6FA33E97F12A

SILC Phase	Timing of Delivery	Deliverable	Deliverable Definition	Acceptance Criteria	Deliverable Classification
Design	Pre-Go Live	12. Infrastructure Plan	The detailed design of how the solution will be implemented either on premise or in the cloud. Specifies: 1. The technologies, sizes and connections of the hosting platform, servers and network infrastructure (if applicable) 2. A Capacity and Performance Plan showing how those technologies will achieve the volume and performance requirements. 3. The deployment model, network topology, and System Architecture Design Document. Includes the STS Solution Design Package for on-premises hosting, or a Cloud Design Package for cloud hosting. May contain the following artifacts defined in the EA Modeling Standard: Deployment Model, Network Topology.	Validation that: 1. The deliverable is in accordance with the contact defined in the deliverable definition and with the deliverable expectation document.	Type C
Design Implementation Operations & Maintenance	Pre-Go Live	13. Master Data Management Plan	The Master Data Management Plan includes approach, strategy, architecture, methodology, process, tools, resourcing, quality and contingency aspects. The MDM Plan shall make data available to integrate with TennCare's project management tools and support ongoing alignment with TennCare Data Policies and Standards and maintain compliance as these standards evolve. The MDM Plan will include the Master and Reference Data design and how it will be created, modified, deleted, accessed, and utilized as defined by the TennCare Data Policies and Standards.	Validation that: 1. The deliverable is in accordance with the contract defined in the deliverable definition and with the deliverable expectation document.	Type C
Test Operations & Maintenance	Pre-Go Live	14. System Security Plan (SSP)	Utilizing the TennCare System Security Plan template (based on the CMS MARS-E standard), documents the strategies and state policies for handling privacy, security, and HIPPA compliance. Contains: 1. Completion of Part A – System Identification a. Executive summary providing a short, high-level description appropriate for achieving an executive-level understanding of what the system is, what sensitive data it processes, and what key protections have been applied; b. System identification providing an overall description of the business process(es) associated with the IT system and an overall description of the IT system environment supporting the business function. 2. Completion of Part B – Security Controls a. Implementation descriptions of the integrated security controls detailing how the system addresses the requirements and standards 3. Completion of Part C – Privacy Controls a. Implementation descriptions of the integrated privacy controls detailing how the system addresses the requirements and standards b. Each SSP must include a response for three entities at a minimum: TennCare, STS, and the system-specific implementation responses. 4. Completion of Part D – SSP Attachments a. Equipment listing consistent with CM-8 (Configuration Management as per NIST 800-53) that supports the system/application b. Software listing consistent with (Configuration Management as per NIST 800-53) that supports the system/application c. Detailed configuration settings consistent with CM-2 (Configuration Management as per NIST 800-53) and CM-6 (Configuration Management as per NIST 800-53) that satisfy the required CMS baseline configurations d. SSP acronyms and abbreviations used in the SSP that are not defined in MARS-E e. SSP glossary containing terms used in the SSP that are not defined in MARS-E	Validation that: 1. The submitted schedule is in alignment with and addresses the requirements defined in the deliverable expectations document and the deliverable definition.	Type D

Docusign Envelope ID: 40B7BFA4-E1BB-4360-9C9C-6FA33E97F12A

SILC Phase	Timing of Delivery	Deliverable	Deliverable Definition	Acceptance Criteria	Deliverable Classification
			5. Additional Artifacts as detailed in Table B-1. MARS-E Security and Privacy Agreements and Compliance Artifacts which includes MARS-E documentation of detailed system security posture and control implementation descriptions. May contain the Security Boundary Model as defined in the EA Modeling Standard.		
Design	Pre-Go Live	15. Data Management Plan	Will contain data conversion logical/technical architecture, including: 1. Mapping documents with associated business rules, strategy to profile, clean, and consolidate data. 2. The Data Transformation Mapping as defined in the EA Modeling Standard. 3. The design for data quality measures including Data Accuracy/Correctness, Completeness, Timeliness/Currency, Consistency/Uniqueness, Validity, Accessibility as defined by the TennCare Data Policies and Standards. 4. The approach, strategy, and architecture for using existing or creating new master and reference data as defined by the TennCare Data Policies and Standards.	Validation that: 1. The plan shall describe the assumptions/constraints/risks related to the data conversion 2. The plan shall describe the strategy related to the data conversion which includes the conversion scope, conversions approach, roles and responsibilities (RACI), Conversion Schedule, Data Quality Controls 3. The plan shall describe the process for data conversion preparation which includes prerequisites, backup strategy and restore process 4. The plan shall describe data conversion specifications which includes data dictionaries and data mappings	Type B
Design	Pre-Go Live	16. Project Change Management Plan	Identification of a change control board along with primary and backup members assigned. Contains: 1. Categorization of change types (e.g., standard, emergency, etc.) 2. Processes for requesting, tracking, and performing impact analyses for each change request 3. Processes for deciding whether to approve changes and for verifying that changes were made correctly	Validation that: 1. The plan is developed in accordance with the TennCare Information Systems Lifecycle 2. The plan is developed in accordance with the Change Management Standard 3. Project Change Management Plan aligns with and is approved by TennCare's Enterprise Change Management Processes 4. Change Management Plan DED has been created and approved by	Type B

Docusign Envelope ID: 40B7BFA4-E1BB-4360-9C9C-6FA33E97F12A

SILC Phase	Timing of Delivery	Deliverable	Deliverable Definition	Acceptance Criteria	Deliverable Classification
				TennCare 5. Simultaneous approval of the Configuration and Deployment Management Plan, Contract Management Plan, and Organizational Change Management (OCM) Plan. 6. Simultaneous approval of the Project Change Request Template	
Development	Pre-Go Live	17. Unit Test Report	Unit Test Cases, Scripts, Data, Results & Mitigation Plan Declares that the solution vendor has completed the Unit Testing stage for a module. It indicates: 1. What module version was tested, with what data on what environment 2. The percentage of test cases passed, failed, and not completed 3. The number of defects outstanding, by severity 4. The mitigation plan for each outstanding defect	Validation that: 1. The Unit and Connectivity test cases are approved (as an appropriate and complete set) 2. 100% of approved Unit and Connectivity test cases are tested (completed) 3. Threshold % of Unit and Connectivity test cases are successful (passed) (the threshold percentage is to be defined in the RFP, Contract, or approved Module Test Plan) 4. All defects have been logged in the defect management tool with a severity level 5. Defects are fixed where feasible 6. All unresolved defects have a mitigation plan approved by TennCare	Type B
Development	Pre-Go Live	18. Implementation Plan	The detailed steps that will be required to implement the solution into production from the development cycle, including processes, resources, roles and responsibilities, support during deployment, confirmation that data is available and accurate, and the transition to the operating organization. The Implementation Plan must include a bill of materials for what will be implemented, describing what the solution contains e.g., software components, technology components and tools, backup technologies and server/storage, etc.	Validation that: 1. The Implementation Plan addresses the required activities and are sequenced accordingly, with defined roles and responsibilities. 2. The plan shall describe the assumptions/constraints/risks related to the implementation approach 3. The plan shall describe	Type B

Docusign Envelope ID: 40B7BFA4-E1BB-4360-9C9C-6FA33E97F12A

SILC Phase	Timing of Delivery	Deliverable	Deliverable Definition	Acceptance Criteria	Deliverable Classification
				the phased approach focusing on costs and longer term goal for the project across all workstreams 4. The plan shall include the project scope, approach and resource plan 5. The plan shall describe a bottom-up approach to calculate the development effort and team structure that derives from the resource plan	
Development	Pre-Go Live	19. Business Continuity/Disaster Recovery Plan	The detailed processes, techniques and activities that are required to continue routine business operations in the event of a disaster. This plan defines: 1. The processes and procedures for business continuation, including: a. key staff b. required equipment 2. Disaster recovery plans for the solution, communications, hardware, and any IT assets (if applicable) 3. Analysis of potential threats 4. Areas of responsibility 5. Emergency contact information 5. Recovery Teams 6. Data and Solution Recovery 7. Communications Strategy 8. Identification and Backup of Essential Services 9. Recovery to pre-disaster state	Validation that: 1. The BC/DR contain detailed processes and activities required to operate the business in the event of a disaster 2. The detailed processes and steps for recovering solutions to a pre-disaster state	Type C
Development	Pre-Go Live	20. Incident Management Plan	Defines: 1. What constitutes an Incident, Incident classifications, Severity Levels, and target times for resolution 2. Processes for reporting, logging, managing, and tracking Incidents to resolution and closure 3. Process for communicating with affected Stakeholders 4. Identification of an Incident manager 5. Determining criteria for creating Problems from Incidents 6. Event Management Plan 7. Problem Management Plan 8. System Incident and Corrective Maintenance Reports 9. Contains Contractor's general contact information for Incident notification and specific individual(s) with roles to contact in the event of a security or privacy Incident. 10. Describes how the Contractor will communicate and notify TennCare Security and Privacy regarding Incidents from Incident inception through resolution. 11. Corresponds to the Incident Response Plan that meets federal, State of Tennessee, and TennCare contractual requirements for the Data Types contained (CMS template available).	Validation that: 1. The Incident Management Plan contains detailed definitions and processes for the identification, categorization, mitigation, and reporting of encountered Incidents. 2. Additionally, the plan contains comprehensive details related to event and Problem management.	Type B

Docusign Envelope ID: 40B7BFA4-E1BB-4360-9C9C-6FA33E97F12A

SILC Phase	Timing of Delivery	Deliverable	Deliverable Definition	Acceptance Criteria	Deliverable Classification
Development	Pre-Go Live	21. Security Management Plan	The Security Management Plan is a planning phase Security deliverable that describes how a project team or vendor plans to staff and manage Security activities for the project Implementation and O&M. This is used at the very beginning of the project to ensure that proper resources, functions, and teams are being properly aligned specific to supporting the successful security and privacy of the project. This document should include at minimum the below sections. A more detailed Template is located on the TennCare Security Intranet site (template in development). 1. Scope 2. Descriptions, Objectives, and Methodology 3. Contracts, Statement of Work, Control Letters 4. Planned Deliverables 5. Staffing Roles and Responsibilities 6. Contacts 7. Training 8. Incident Response Coordination 9. Current or Planned Certifications 10. Key Milestones 11. Subcontractors	Validation that: 1. Information in the Security Management Plan Template meets or exceeds the required fields identified in the template.	Type B
Test	Pre-Go Live	22. System Integration Test (SIT) Report	Contains: 1. Test Cases 2. Test Data 3. Test Scripts 4. Test Reports 5. Test Summary Report 6. Defects & Mitigation	Validation that: 1. The System Integration Test (SIT) test cases are approved (as an appropriate and complete set) 2. 100% of approved SIT test cases are tested (completed) 3. All critical and blocking defects (from SIT or previous stages) have been resolved 4. All unresolved defects have a mitigation plan approved by TennCare	Type B
Test	Pre-Go Live	23. User Acceptance Test (UAT) Report	Contains: 1. Acceptance testing report for each user story/use case 2. Formal Acceptance Testing Report 3. System Readiness Certification for UAT 4. Test Reports 5. Test Summary Report 6. Unit, System, and Integration Testing Test Results 7. Automated Code Review Results	Validation that: 1. The UAT test cases are approved (as an appropriate and complete set) 2. 100% of approved UAT test cases are tested (completed) 3. All critical and blocking defects (from UAT or previous stages) have been resolved 4. All unresolved defects have a mitigation plan approved by TennCare 5. The TennCare UAT	Type B

Docusign Envelope ID: 40B7BFA4-E1BB-4360-9C9C-6FA33E97F12A

SILC Phase	Timing of Delivery	Deliverable	Deliverable Definition	Acceptance Criteria	Deliverable Classification
				testing team accepts the solution module	
Test Operations & Maintenance	Pre-Go Live	24. Privacy Impact Assessment	Utilizes CMS template for overall privacy analysis of the system. The PIA applies to a single system, and the analysis is completed based upon the privacy within the security boundary of the system being implemented.	Validation that: 1. The Privacy Impact Analysis (PIA) only documents a single system contained within a single security boundary. The PIA may NOT contain multiple system across security boundaries. 2. The CMS Privacy Impact Assessment (PIA) Template that has all response fields completed with accurate and comprehensive responses	Type C
Test Operations & Maintenance	Pre-Go Live	25. Information Security Risk Assessment	Utilizes CMS template report for Risks as a result of an identified Weakness [Plane of Action & Milestone (POAM)] or Risk Acceptance from baseline controls and standards in MARS-E. As part of an iterative document development process, the documents note business and technical risks starting near the completion of the design process and continues until the system is ready to be placed into production. The first final submission is part of the ATO package and updated annually or in the event of a significant system change thereafter, whichever comes first.	Validation that: 1. The CMS Information Security Risk Assessment (ISRA) Procedure have accurately been followed and that has all response fields completed with accurate and comprehensive responses. 2. The ISRA shall document security, privacy and business risks related to the operation and use of the system. 3. Describes the implementation of effective and timely controls and mitigation measures to minimize risk exposures including plans for addressing security and privacy risks, documents the risks associated with the system, describes processes to measure and monitor risks associated with the system.	Type C
Implementation	Pre-Go Live	26. Operational Readiness Test (ORT) Report	Each Test Report declares that the solution vendor has completed a stage of testing of a module. It indicates: 1. What module version was tested, with what data on what environment 2. The percentage of test cases passed, failed, and not completed	Validation that: 1. The Operational Readiness Test (ORT) test cases are approved (as an appropriate and complete	Type B

Docusign Envelope ID: 40B7BFA4-E1BB-4360-9C9C-6FA33E97F12A

SILC Phase	Timing of Delivery	Deliverable	Deliverable Definition	Acceptance Criteria	Deliverable Classification
			3. The number of defects outstanding, by severity 4. The mitigation plan for each outstanding defect	set) 2. 100% of approved ORT test cases are test (completed) 3. All critical and blocking defects (from ORT or previous stages) have been resolved 4. All unresolved defects have a mitigation plan approved by TennCare 5. The TennCare IS testing team accepts the solution module	
Implementation	Post Go Live Last 180 days of Contract Term	27. Turnover Plan	Documentation that describes how a solution is transitioned to another vendor or to TennCare for continued operation. The plan will include: 1. Data Turnover tasks; 2. Custom Interface turnover tasks; 3. Reusable code, configurations, and turnover tasks; 4. Documentation regarding products (with versions), files, interfaces, and work flows not considered to be part of the COTS proprietary documentation tasks; and 5. A timeline with milestones for the Turnover to include planning, execution, and implementation approval.	Validation that: 1. The plan contains a list of all tasks, timeline and milestones required to perform the turnover 2. The plan contains complete documentation of the solution as described in the deliverable definition	Type C
Implementation Operations & Maintenance	Post Go Live	28. Operations & Maintenance Run Book	Product documentation that describes how to operate the solution. Contains: 1. Operations manuals 2. Standard operating procedures (SOP) 3. User guides 4. List of all error codes and explanations by component 5. Infrastructure Services Deployment Report 6. Infrastructure, System Source Code, and Documentation 7. Manuals and Training Materials 8. Operations & Support procedures 9. System Configuration Document 10. Interface Descriptions/Controls including data flow between modules and repositories 11. System Operations Documentation 12. Training Artifacts 13. Training Plan 14. Updated Infrastructure System Source Code and Documentation 15. A substantive and representative set of all reports and information retrieval screens (electronic format preferred) 16. A list of information retrieval functions and reports for each business area (including a list that identifies the distribution of the reports and who can access the information retrieval displays) 17. Plan for rolling out the new or updated module/system to the users 18. Implementation and Deployment Plan 19. Performance, Availability and Capacity Plan 10. Release and Deployment Plan 21. Service Transition Plan 22. System Maintenance, Support, and System Transition Plan	Validation that: 1. The submitted deliverable is in alignment with and addresses the requirements defined in the deliverable expectations document and the deliverable definition.	Type C

Docusign Envelope ID: 40B7BFA4-E1BB-4360-9C9C-6FA33E97F12A

SILC Phase	Timing of Delivery	Deliverable	Deliverable Definition	Acceptance Criteria	Deliverable Classification
			23. Cutover Plan 24. Description of how data should be created and maintained including Data Corrections, Data Retirement, Purge, Archive, and Retention, Data Quality controls and monitors, and data history capture and audit processes and data structures implemented to capture audit information (will also be captured in Physical Data Dictionary)		
Implementation	Post Go Live	29. Authority to Operate (ATO)	Formal signoff by TennCare Business/System Owner acknowledging they have performed their diligence for Privacy, Security, and Operations and authorizing production to go live.	Validation that: 1. All initial security and privacy documentation and test are completed and approved.	Type A
Implementation Operations & Maintenance	Post Go Live	30. Security Assessment Plan	This Security and Privacy Assessment Plan (SAP) documents all testing to validate the security and privacy controls for a system. The Security Assessment Plan must be delivered to CMS a minimum of 60 days prior to the kickoff of the Third-Party Independent Assessment. The plan is completed by the third party assessor for the benefit of TennCare and federal regulators. Following the Framework for Independent Assessment of Security and Privacy Controls the assessment plan documents how the assessor will evaluate: 1. System compliance with security & privacy controls in the SSP 2. Underlying infrastructure's security posture 3. The system and data security and privacy posture 4. Proper security configuration associated with the database or file structure storing the data 5. Systems technical, managerial, and organizational adherence to the organization's security and privacy program, policies, and guidance	Validation that: 1. The full assessment report, associated report, and findings are provided to TennCare security and privacy teams. 2. The security and privacy teams agree that the assessment tested the right items, performed a thorough scan of all these items, and that the report accurately reflects this. 3. Any minimal security/privacy risks that were found are being remediated and the remediation plan is being reported on to TennCare.	Type C
Implementation Operations & Maintenance	Post Go Live	31. Independent Security Audti	The purpose of a Security Control Assessment (SCA) is to determine whether the security and privacy controls are implemented correctly, operate as intended, and produce the desired outcomes for meeting the security and privacy requirements of the application or system. The SCA also identifies areas of risk that require the State's attention and remediation. Independent review as defined by CMS of control effectiveness using SSP Control Set and NIST 800-53A review methods with required guidance from CMS MARSE template and guidance on conducting "Independent Third-Party Security and Privacy Audit Guidelines for Medicaid Enterprise System (MES) Certification. The third-party security and privacy assessor must be free from any real or perceived conflicts of interest, including being free from personal, external, and organizational impairments to independence, or the appearance of such impairments to independence. An assessor is considered independent if there is no perceived or actual conflict of interest involving the developmental, operational, financial , and/or management chain associated with the system and the determination of security and privacy control effectiveness.	Validation that: 1. The full assessment report, associated report, and findings are provided to TennCare security and privacy teams. 2. The security and privacy teams agree that the assessment tested the right items, performed a thorough scan of all these items, and that the report accurately reflects this. 3. Any minimal security/privacy risks that were found are being remediated and the	Type C

Docusign Envelope ID: 40B7BFA4-E1BB-4360-9C9C-6FA33E97F12A

SILC Phase	Timing of Delivery	Deliverable	Deliverable Definition	Acceptance Criteria	Deliverable Classification
			At the completion of the assessment, the assessor provides a Security and Privacy Assessment Report (SAR) to TennCare's Business Owner, who is then responsible for providing the report to CMS. The SAR content includes the following information: 1. System Overview 2. Executive Summary Report 3. Detailed Findings Report 4. Scan Results: i. Infrastructure Scan ii. Database Scan iii. Web Application Scan 5. Penetration Test Report 6. Penetration Test and Scan Results Summary	remediation plan is being reported on to TennCare.	
Implementation Operations & Maintenance	Post Go Live	32. Plan of Actions and Milestones	Plans of Actions and Milestones: At the latest is created and reported upon completion of the Security Assessment Report detailing remediation of any "planned" control actions or assessment findings needing remediation. These findings are logged, tracked and updated in the TennCare electronic Governance Risk and Compliance system on a monthly basis by the vendor. These may be temporarily tracked using the CMS provided POAM spreadsheet with the approval of the TennCare Chief Security Officer.	Validation that: 1. Risk and findings are logged in the CMS POAM format within the TennCare Governance Risk and Compliance (GRC) system. 2. Vendor completes monthly updates to all POAM's after initial submission 3. Vendor attends monthly POAM meetings with TennCare Security,	Type B
Implementation Operations & Maintenance	Post Go Live	33. Third-Party Security and Privacy Assessment	The purpose of a Security Control Assessment (SCA) is to determine whether the security and privacy controls are implemented correctly, operate as intended, and produce the desired outcomes for meeting the security and privacy requirements of the application or system. The SCA also identifies areas of risk that require the State's attention and remediation. Independent review as defined by CMS of control effectiveness using SSP Control Set and NIST 800-53A review methods with required guidance from CMS MARSE template and guidance on conducting "Independent Third-Party Security and Privacy Audit Guidelines for Medicaid Enterprise System (MES) Certification. The third-party security and privacy assessor must be free from any real or perceived conflicts of interest, including being free from personal, external, and organizational impairments to independence, or the appearance of such impairments to independence. An assessor is considered independent if there is no perceived or actual conflict of interest involving the developmental, operational, financial, and/or management chain associated with the system and the determination of security and privacy control effectiveness. At the completion of the assessment, the assessor provides a Security and Privacy Assessment Report (SAR) to TennCare's Business Owner, who is then responsible for providing the report to CMS. The SAR content includes the following information: 1. System Overview	Validation that: 1. The full assessment report, associated report, and findings are provided to TennCare security and privacy teams. 2. The security and privacy teams agree that the assessment tested the right items, performed a thorough scan of all these items, and that the report accurately reflects this. 3. Any minimal security/privacy risks that were found are being remediated and the remediation plan is being reported on to TennCare.	Type C

Docusign Envelope ID: 40B7BFA4-E1BB-4360-9C9C-6FA33E97F12A

SILC Phase	Timing of Delivery	Deliverable	Deliverable Definition	Acceptance Criteria	Deliverable Classification
			2. Executive Summary Report 3. Detailed Findings Report 4. Scan Results: i. Infrastructure Scan ii. Database Scan iii. Web Application Scan 5. Penetration Test Report 6. Penetration Test and Scan Results Summary		
Requirements Review Design Development Test Implement Operations & Maintenance	Post Go Live Every month by end of last business day	34. Monthly Project Status Reports	Indicators of Project Health, which are: 1. Roadmap - A product roadmap identifying current, planned, and future functionality and milestones. 2. Progress Tracking - A regular report measuring development progress and progress towards achieving outcomes. 3. User Feedback - A reporting showing how user feedback is regularly incorporated into development. 4. Defect and Risk List - Known defects and risks that may cause delays and any mitigations or workarounds. 5. Product Demos - Demo of functionality/features, or regular report of code/feature releases. 6. Testing Process - A documented testing process aligned with the Testing Guidance Framework.	Validation that: 1. The Monthly Project Status Report is in alignment with CMS Standards.	Type A
Operations & Maintenance	Post Go Live	35. Contingency Plan	Standard NIST based methods for documenting Continuity and Disaster Planning as defined in SP 800-34.	Validation that: 1. Information contained in the plan meets or exceeds the standards in NIST SP 800-34 2. The Contingency Plan meets or exceeds the requirements in the current version of MARS-E Contingency Planning (CP) family of security controls, control enhancements, and implementation standards as defined in the System Security Plan template as applicable. 3. The Contingency Plan meets or exceeds the requirements in the current version of MARS-E related control requirements for the Contingency Planning (CP). These are listed in the "Related Control Requirement(s) section of the System Security Plan Template	Type C

Docusign Envelope ID: 40B7BFA4-E1BB-4360-9C9C-6FA33E97F12A

SILC Phase	Timing of Delivery	Deliverable	Deliverable Definition	Acceptance Criteria	Deliverable Classification
Operations & Maintenance	Post Go Live	36. Metrics Report	Module-Specific metrics that demonstrate the system is meeting business objectives. Metrics that provide evidence that the outcomes are met on an ongoing basis. In accordance with 42 C.F.R. §433.112(b)(15) and §433.116(b), (c), and (i), states must be capable of producing: 1. Data 2. Reports 3. Performance information from and about their MES modules All of which will be used to facilitate evaluation, continuous improvement in business operations, and transparency and accountability, as a condition for receiving enhanced federal matching for MES expenditures. The IS Solution Vendor will produce enterprise or IS-level data and reports for metrics reporting.	Validation that: 1. Metric reporting can be completed with appropriate results generated by the DDI vendor. 2. TennCare owners have signed off on each metric result to be reported	Type A
Retire	Post Go Live	37. System Disposition Plan / Report	Documents how the various components of an automated system (software, data, hardware, communications, and documentation) are to be handled at the completion of operations to ensure proper disposition of all the system components and to avoid disruption of the individuals and/or other systems impacted by the disposition	Validation that: 1. The solution/system has been successfully disposed in accordance with the System Disposition Plan 2. TennCare has approved the System Disposition Report and verified that the appropriate activities have taken place: a. The system is properly shutdown b. Project archives are located in the correct place and on the correct medium c. System security and data procedures were followed correctly to ensure the protection of private or sensitive data and that there is no user access to the system/application/solution d. Any continued use of system or application components are done in accordance within State security requirements and are fully documented in the System Disposition Report e. Final phase-end review has been conducted after the system retirement to ascertain if the system and data have been	Type C

Docusign Envelope ID: 40B7BFA4-E1BB-4360-9C9C-6FA33E97F12A

SILC Phase	Timing of Delivery	Deliverable	Deliverable Definition	Acceptance Criteria	Deliverable Classification
				completely and appropriately disposed of f. Security objectives, including secure data and system transfer, sanitization and disposal of media has been accomplished g. Project Archives that preserve vital information, including both documentation of project execution and the data from the production system has been appropriately preserved	
Operations & Maintenance	Post Go Live Quarterly	38. SOC Monitoring Status Report	The contractor shall supply TennCare with a report detailing the status of the SOC, analyzing strengths and weaknesses with any planned improvements or changes	Validation that the report is completed with all applicable contents and approval from TennCare Security leadership.	Type A
Operations & Maintenance	Post Go Live 3rd business day of each month	39. SEIM Content Pipeline Report	The contractor shall supply TennCare with a report summarizing all applicable SEIM content with actionable steps to improve the organization's security posture	Validation that the report is completed with all applicable contents and approval from TennCare Security leadership.	Type A
Operations & Maintenance	Post Go Live Weekly	40. Threat Intel Report	The contractor shall supply TennCare with a report detailing any threats currently facing TennCare and the Medicare/Medicaid industry overall	Validation that the report is completed with all applicable contents and approval from TennCare Security leadership.	Type A
Operations & Maintenance	Post Go Live Monthly	41. Alert Matrix Report	The contractor shall supply TennCare with a monthly report with a matrix detailing the threats facing TennCare and the Medicare/Medicaid industry with the relevant level of risk and complexity	Validation that the report is completed with all applicable contents and approval from TennCare Security leadership.	Type A
Operations & Maintenance	Post Go Live 3rd business day of each month	42. SLA Compliance Report	The contractor shall provide TennCare with a report detailing the compliance with and/or status of all applicable Service Level Agreements	Validation that report is completed by the vendor and that all current SLAs are in compliance, or any non-compliant items have justifications and remediation steps Acknowledgement of justification and compliance by TennCare leadership	Type A

Docusign Envelope ID: 40B7BFA4-E1BB-4360-9C9C-6FA33E97F12A

SILC Phase	Timing of Delivery	Deliverable	Deliverable Definition	Acceptance Criteria	Deliverable Classification
Operations & Maintenance	Post Go Live Bi-Weekly	43. Bi- Weekly False Positive Tickets Report	The contractor shall provide TennCare with a bi-weekly report detailing all false positive tickets and all appropriate responses and/or remediations	Validation that the report is completed with all applicable contents and approval from TennCare Security leadership.	Type A
Operations & Maintenance	Post Go Live Quarterly	44. Quarterly Business Report	The contractor shall provide TennCare an executive summary of all actions taken within the past quarter, in progress, and any upcoming plans, changes, or modifications within the scope of the services provided to TennCare	Validation that the report is completed with all applicable contents and approval from TennCare Security leadership.	Type A
Operations & Maintenance	Post Go Live Weekly, BeginningYear 2 of Agreement Term	45. Threat Hunting Report	The contractor shall supply TennCare with a weekly report containing any possible threats, anomalies, and any other malicious activities that may affect TennCare or TennCare supporting infrastructure	Validation that the report is completed with all applicable contents and approval from TennCare Security leadership.	Type A
Operations & Maintenance	Post Go Live To be defined by TennCare	46. Major Incident Report	For major incidents with incident summary, the contractor shall provide comprehensive details on the findings and remediation steps taken, root cause analysis, and recommendations for future Solution hardening.	Validation that the report is completed with all applicable contents and approval from TennCare Security leadership.	Type A
Operations & Maintenance	Post Go Live To be defined by TennCare	47. User and Entity Behavior Analytics	User and Entity Behavior Analytics (UEBA) including, but not limited to, identifying, triaging, and alerting on privileged account abuse, privilege escalation, data exfiltration, anomalous behavior, and credential compromise, in a format and cadence to be defined by TennCare	Validation that the report is completed with all applicable contents and approval from TennCare Security leadership.	Type A

B. TERM OF CONTRACT:

B.1. This Contract shall be effective on April 1, 2025 ("Effective Date") and extend for a period of thirty-six (36) months after the Effective Date ("Term"). The State shall have no obligation for goods or services provided by the Contractor prior to the Effective Date.

B.2. Renewal Options. This Contract may be renewed upon satisfactory completion of the Term. The State reserves the right to execute up to two (2) renewal options under the same terms and conditions for a period not to exceed twelve (12) months each by the State, at the State's sole option. In no event, however, shall the maximum Term, including all renewals or extensions, exceed a total of sixty (60) months.

C. PAYMENT TERMS AND CONDITIONS:

C.1. Maximum Liability. In no event shall the maximum liability of the State under this Contract exceed Four Million Seven Hundred Seventeen Thousand Dollars ($4,717,000.00) ("Maximum Liability"). This Contract does not grant the Contractor any exclusive rights. The State does not guarantee that it will buy any minimum quantity of goods or services under this Contract. Subject to the terms and conditions of this Contract, the Contractor will only be paid for goods or services provided under this Contract after a purchase order is issued to Contractor by the State or as otherwise specified by this Contract.

C.2. Compensation Firm. The payment methodology in Section C.3. of this Contract shall constitute the entire compensation due the Contractor for all goods or services provided under this Contract regardless of the difficulty, materials or equipment required. The payment methodology includes all applicable taxes, fees, overhead, and all other direct and indirect costs incurred or to be incurred by the Contractor.

C.3. Payment Methodology. The Contractor shall be compensated based on the payment methodology for goods or services in Attachment G, Cost Proposal and as authorized by the State in a total amount as set forth in Section C.1.

a) The Contractor's compensation shall be contingent upon the satisfactory provision of goods or services as set forth in Section A.

b) The Contractor shall be compensated based upon the following payment methodology:

Quarterly Payment	Amount (per compensable increment)
Year 1 (Annual Cost)	$ 1,665,000.00
Quarters 1 - 4	25% each quarter of Year 1
Year 2 (Annual Cost)	$ 1,572,000.00
Quarters 1 - 4	25% each quarter of Year 2
Year 3 (Annual Cost)	$ 1,480,000.00
Quarters 1 - 4	25% each quarter of Year 3
Total Base Years	$ 4,717,000.00

In the event that the State renews this Contract in accordance with B.2., the Contractor shall be compensated based on the following payment methodology.

Docusign Envelope ID: 40B7BFA4-E1BB-4360-9C9C-6FA33E97F12A

Quarterly Payment	Amount (per compensable increment)
Extension Year 1	$ 1,387,500.00
Quarters 1 - 4	25% each quarter of Extension Year 1
Extension Year 2	$ 1,387,500.00
Quarters 1 - 4	25% each quarter of Extension Year 2

c) The Contractor shall be compensated for Special Project Change Orders and Enhancement Change Orders requested and performed pursuant to Contract Section A.12.5. without a formal amendment of this Contract based upon the allocated amount in the Special Projects and Enhancement funds detailed in Contract Attachment G, Cost Proposal, PROVIDED THAT:

1) Compensation to the Contractor for Special Project Change Orders shall not exceed ten percent (10%) the sum of the Total Base Yearly Costs above.

   a. Special Project Change Orders shall be paid upon the successful unconditional pass of the associated Gate Review and TennCare Acceptance of all associated Deliverables.

   b. All Special Projects shall be associated with a Gate Review as determined by TennCare and not paid until approved as part of the Gate Review process.

2) Compensation to the Contractor for Enhancement Change Orders shall not exceed the cost associated with ten percent (10%) of the sum of the Total Base Yearly Cost.

   a. Enhancement Change Orders shall be paid upon successful release of the enhancement functionality as determined by TennCare, in its sole discretion.

3) If, at any point during the Term, the State determines that the cost of necessary Special Projects and Enhancements work would exceed the maximum amount, the State may amend this Contract to address the need.

Service Description	Amount (per compensable increment)
Total Special Project Change Order Requests compensation	**$ 471,700.00 (10% of the Total Base Yearly Costs)**
Total Enhancement Change Order Requests compensation	**$ 471,700.00 (10% of the Total Base Yearly Costs)**

C.4. Travel Compensation. The Contractor shall not be compensated or reimbursed for travel time, travel expenses, meals, or lodging.

C.5. Invoice Requirements. The Contractor shall invoice the State only for goods delivered and accepted by the State or services satisfactorily provided at the amounts stipulated in Section C.3, above. All invoices submitted for any and all services rendered by Contractor's staff and subcontractors (resource reporting), the invoice shall, at a minimum, include the name of each individual, the individual's role classification, the number of hours worked during the period, the applicable Payment Rate, the total compensation requested for the individual, and the total amount due the Contractor for the period invoiced. Contractor shall submit invoices and necessary supporting documentation, no more frequently than once a month, and no later than thirty (30) days after goods or services have been provided to the following address:

Division of TennCare

Docusign Envelope ID: 40B7BFA4-E1BB-4360-9C9C-6FA33E97F12A

310 Great Circle Road
Nashville, TN 37243

a) Each invoice, on Contractor's letterhead, shall clearly and accurately detail all of the following information (calculations must be extended and totaled correctly):

1) Invoice number (assigned by the Contractor);

2) Invoice date;

3) Contract number (assigned by the State);

4) Customer account name: Department of Finance and Administration, Division of TennCare;

5) Customer account number (assigned by the Contractor to the above-referenced Customer);

6) Contractor name;

7) Contractor Tennessee Edison registration ID number;

8) Contractor contact for invoice questions (name, phone, or email);

9) Contractor remittance address;

10) Description of delivered goods or services provided and invoiced, including identifying information as applicable;

11) Number of delivered or completed units, increments, hours, or days as applicable, of each good or service invoiced;

12) Applicable payment methodology (as stipulated in Section C.3) of each good or service invoiced;

13) Amount due for each compensable unit of good or service; and

14) Total amount due for the invoice period.

b) Contractor's invoices shall:

1) Only include charges for goods delivered or services provided as described in Section A and in accordance with payment terms and conditions set forth in Section C;

2) Only be submitted for goods delivered or services completed and shall not include any charge for future goods to be delivered or services to be performed;

3) Not include Contractor's taxes, which includes without limitation Contractor's sales and use tax, excise taxes, franchise taxes, real or personal property taxes, or income taxes; and

4) Include shipping or delivery charges only as authorized in this Contract.

c) The timeframe for payment (or any discounts) begins only when the State is in receipt of an invoice that meets the minimum requirements of this Section C.6.

C.6. Payment of Invoice. A payment by the State shall not prejudice the State's right to object to or question any payment, invoice, or other matter. A payment by the State shall not be construed as acceptance of goods delivered, any part of the services provided, or as approval of any amount invoiced.

C.7. Invoice Reductions. The Contractor's invoice shall be subject to reduction for amounts included in any invoice or payment that is determined by the State, on the basis of audits conducted in

Docusign Envelope ID: 40B7BFA4-E1BB-4360-9C9C-6FA33E97F12A

accordance with the terms of this Contract, to not constitute proper compensation for goods delivered or services provided.

C.8. Deductions. The State reserves the right to deduct from amounts, which are or shall become due and payable to the Contractor under this or any contract between the Contractor and the State of Tennessee, any amounts that are or shall become due and payable to the State of Tennessee by the Contractor.

C.9. Prerequisite Documentation. The Contractor shall not invoice the State under this Contract until the State has received the following, properly completed documentation.

a. The Contractor shall complete, sign, and present to the State the "Authorization Agreement for Automatic Deposit Form" provided by the State. By doing so, the Contractor acknowledges and agrees that, once this form is received by the State, payments to the Contractor, under this or any other contract the Contractor has with the State of Tennessee, may be made by ACH; and

b. The Contractor shall complete, sign, and return to the State the State-provided W-9 form. The taxpayer identification number on the W-9 form must be the same as the Contractor's Federal Employer Identification Number or Social Security Number referenced in the Contractor's Edison registration information.

D. MANDATORY TERMS AND CONDITIONS:

D.1. Required Approvals. The State is not bound by this Contract until it is duly approved by the Parties and all appropriate State officials in accordance with applicable Tennessee laws and regulations. Depending upon the specifics of this Contract, this may include approvals by the Commissioner of Finance and Administration, the Commissioner of Human Resources, the Comptroller of the Treasury, and the Chief Procurement Officer. Approvals shall be evidenced by a signature or electronic approval.

D.2. Communications and Contacts. All instructions, notices, consents, demands, or other communications required or contemplated by this Contract shall be in writing and shall be made by certified, first-class mail, return receipt requested and postage prepaid, by overnight courier service with an asset tracking system, or by email or facsimile transmission with recipient confirmation. All communications, regardless of method of transmission, shall be addressed to the respective Party at the appropriate mailing address, facsimile number, or email address as stated below or any other address provided in writing by a Party.

The State:

Deputy Commissioner
Department of Finance and Administration
Division of TennCare
310 Great Circle Road
Nashville, TN 37243
Telephone # 615-507-6443
FAX # 615-253-5607

The Contractor:

Amit Gandre, CEO Americas
Inspira Enterprise, Inc.
1301 Solana Blvd., Suite 2570
Westlake, TX 76262
amit.gandre@inspiraenterprise.com
Telephone # 813-428-4530

Docusign Envelope ID: 40B7BFA4-E1BB-4360-9C9C-6FA33E97F12A

Vishal Jain, Co-founder, Managing Director
Inspira Enterprise, Inc.
1301 Solana Blvd., Suite 2570
Westlake, TX 76262
vishal.jain@inspiraenterprise.com
Telephone # 254-467-7472

All instructions, notices, consents, demands, or other communications shall be considered effective upon receipt or recipient confirmation as may be required.

D.3. Modification and Amendment. This Contract may be modified only by a written amendment signed by all Parties and approved by all applicable State officials.

D.4. Subject to Funds Availability. The Contract is subject to the appropriation and availability of State or federal funds. In the event that the funds are not appropriated or are otherwise unavailable, the State reserves the right to terminate this Contract upon written notice to the Contractor. The State's exercise of its right to terminate this Contract shall not constitute a breach of Contract by the State. Upon receipt of the written notice, the Contractor shall cease all work associated with the Contract. If the State terminates this Contract due to lack of funds availability, the Contractor shall be entitled to compensation for all conforming goods requested and accepted by the State and for all satisfactory and authorized services completed as of the termination date. Should the State exercise its right to terminate this Contract due to unavailability of funds, the Contractor shall have no right to recover from the State any actual, general, special, incidental, consequential, or any other damages of any description or amount.

D.5. Termination for Convenience. The State may terminate this Contract for convenience without cause and for any reason. The State shall give the Contractor at least thirty (30) days written notice before the termination date. The Contractor shall be entitled to compensation for all conforming goods delivered and accepted by the State or for satisfactory, authorized services completed as of the termination date. In no event shall the State be liable to the Contractor for compensation for any goods neither requested nor accepted by the State or for any services neither requested by the State nor satisfactorily performed by the Contractor. In no event shall the State's exercise of its right to terminate this Contract for convenience relieve the Contractor of any liability to the State for any damages or claims arising under this Contract.

D.6. Termination for Cause. If the Contractor fails to properly perform its obligations under this Contract in a timely or proper manner, or if the Contractor materially violates any terms of this Contract ("Breach Condition"), the State shall have the right to immediately terminate the Contract and withhold payments in excess of compensation for completed services or provided goods. Notwithstanding the above, the Contractor shall not be relieved of liability to the State for damages sustained by virtue of any Breach Condition and the State may seek other remedies allowed at law or in equity for breach of this Contract.

D.7. Assignment and Subcontracting. The Contractor shall not assign this Contract or enter into a subcontract for any of the goods or services provided under this Contract without the prior written approval of the State. Notwithstanding any use of the approved subcontractors, the Contractor shall be the prime contractor and responsible for compliance with all terms and conditions of this Contract. The State reserves the right to request additional information or impose additional terms and conditions before approving an assignment of this Contract in whole or in part or the use of subcontractors in fulfilling the Contractor's obligations under this Contract.

D.8. Conflicts of Interest. The Contractor warrants that no part of the Contractor's compensation shall be paid directly or indirectly to an employee or official of the State of Tennessee as wages, compensation, or gifts in exchange for acting as an officer, agent, employee, subcontractor, or consultant to the Contractor in connection with any work contemplated or performed under this Contract.

The Contractor acknowledges, understands, and agrees that this Contract shall be null and void if

Docusign Envelope ID: 40B7BFA4-E1BB-4360-9C9C-6FA33E97F12A

the Contractor is, or within the past six (6) months has been, an employee of the State of Tennessee or if the Contractor is an entity in which a controlling interest is held by an individual who is, or within the past six (6) months has been, an employee of the State of Tennessee.

D.9. Nondiscrimination. The Contractor hereby agrees, warrants, and assures that no person shall be excluded from participation in, be denied benefits of, or be otherwise subjected to discrimination in the performance of this Contract or in the employment practices of the Contractor on the grounds of handicap or disability, age, race, creed, color, religion, sex, national origin, or any other classification protected by federal or state law. The Contractor shall, upon request, show proof of nondiscrimination and shall post in conspicuous places, available to all employees and applicants, notices of nondiscrimination. This Section D.9 shall not be deemed to limit or abridge any requirement set forth in Section E.34.

D.10. Prohibition of Illegal Immigrants. The requirements of Tenn. Code Ann. § 12-3-309 addressing the use of illegal immigrants in the performance of any contract to supply goods or services to the state of Tennessee, shall be a material provision of this Contract, a breach of which shall be grounds for monetary and other penalties, up to and including termination of this Contract.

a. The Contractor agrees that the Contractor shall not knowingly utilize the services of an illegal immigrant in the performance of this Contract and shall not knowingly utilize the services of any subcontractor who will utilize the services of an illegal immigrant in the performance of this Contract. The Contractor shall reaffirm this attestation, in writing, by submitting to the State a completed and signed copy of the document at Attachment E, semi-annually during the Term. If the Contractor is a party to more than one contract with the State, the Contractor may submit one attestation that applies to all contracts with the State. All Contractor attestations shall be maintained by the Contractor and made available to State officials upon request.

b. Prior to the use of any subcontractor in the performance of this Contract, and semi-annually thereafter, during the Term, the Contractor shall obtain and retain a current, written attestation that the subcontractor shall not knowingly utilize the services of an illegal immigrant to perform work under this Contract and shall not knowingly utilize the services of any subcontractor who will utilize the services of an illegal immigrant to perform work under this Contract. Attestations obtained from subcontractors shall be maintained by the Contractor and made available to State officials upon request.

c. The Contractor shall maintain records for all personnel used in the performance of this Contract. Contractor's records shall be subject to review and random inspection at any reasonable time upon reasonable notice by the State.

d. The Contractor understands and agrees that failure to comply with this section will be subject to the sanctions of Tenn. Code Ann. § 12-3-309 for acts or omissions occurring after its effective date.

e. For purposes of this Contract, "illegal immigrant" shall be defined as any person who is not: (i) a United States citizen; (ii) a Lawful Permanent Resident; (iii) a person whose physical presence in the United States is authorized; (iv) allowed by the federal Department of Homeland Security and who, under federal immigration laws or regulations, is authorized to be employed in the U.S.; or (v) is otherwise authorized to provide services under the Contract.

D.11. Records. The Contractor shall maintain documentation for all charges under this Contract. The books, records, and documents of the Contractor, for work performed or money received under this Contract, shall be maintained for a period of ten (10) full years from the date of the final payment and shall be subject to audit at any reasonable time and upon reasonable notice by the State, the Comptroller of the Treasury, or their duly appointed representatives. The financial statements shall be prepared in accordance with generally accepted accounting principles.

Docusign Envelope ID: 40B7BFA4-E1BB-4360-9C9C-6FA33E97F12A

D.12. Monitoring. The Contractor's activities conducted and records maintained pursuant to this Contract shall be subject to monitoring and evaluation by the State, the Comptroller of the Treasury, or their duly appointed representatives,

D.13. Progress Reports. The Contractor shall submit brief, periodic, progress reports to the State as requested.

D.14. Strict Performance. Failure by any Party to this Contract to require, in any one or more cases, the strict performance of any of the terms, covenants, conditions, or provisions of this Contract shall not be construed as a waiver or relinquishment of any term, covenant, condition, or provision. No term or condition of this Contract shall be held to be waived, modified, or deleted except by a written amendment signed by the Parties.

D.15. Independent Contractor. The Parties shall not act as employees, partners, joint venturers, or associates of one another. The Parties are independent contracting entities. Nothing in this Contract shall be construed to create an employer/employee relationship or to allow either Party to exercise control or direction over the manner or method by which the other transacts its business affairs or provides its usual services. The employees or agents of one Party are not employees or agents of the other Party.

D.16. Patient Protection and Affordable Care Act. The Contractor agrees that it will be responsible for compliance with the Patient Protection and Affordable Care Act ("PPACA") with respect to itself and its employees, including any obligation to report health insurance coverage, provide health insurance coverage, or pay any financial assessment, tax, or penalty for not providing health insurance. The Contractor shall indemnify the State and hold it harmless from any costs to the State arising from Contractor's failure to fulfill its PPACA responsibilities for itself or its employees.

D.17. Limitation of State's Liability. The State shall have no liability except as specifically provided in this Contract. In no event will the State be liable to the Contractor or any other party for any lost revenues, lost profits, loss of business, decrease in the value of any securities or cash position, time, goodwill, or any indirect, special, incidental, punitive, exemplary or consequential damages of any nature, whether based on warranty, contract, statute, regulation, tort (including but not limited to negligence), or any other legal theory that may arise under this Contract or otherwise. The State's total liability under this Contract (including any exhibits, schedules, amendments or other attachments to the Contract) or otherwise shall under no circumstances exceed the Maximum Liability. This limitation of liability is cumulative and not per incident.

D.18. Limitation of Contractor's Liability. In accordance with Tenn. Code Ann. § 12-3-701, the Contractor's liability for all claims arising under this Contract shall be limited to an amount equal to two (2) times the Maximum Liability amount detailed in Section C.1. and as may be amended, PROVIDED THAT in no event shall this Section limit the liability of the Contractor for: (i) intellectual property or any Contractor indemnity obligations for infringement for third-party intellectual property rights; (ii) any claims covered by any specific provision in the Contract providing for Liquidated Damages; or (iii) any claims for intentional torts, criminal acts, fraudulent conduct, or acts or omissions that result in personal injuries or death. For clarity, except as otherwise expressly set forth in this Section, Contractor's indemnification obligations and other remedies available under this Contract are subject to the limitations on liability set forth in this Section.

D.19. Hold Harmless. The Contractor agrees to indemnify and hold harmless the State of Tennessee as well as its officers, agents, and employees from and against any and all claims, liabilities, losses, and causes of action which may arise, accrue, or result to any person, firm, corporation, or other entity which may be injured or damaged as a result of acts, omissions, or negligence on the part of the Contractor, its employees, or any person acting for or on its or their behalf relating to this Contract. The Contractor further agrees it shall be liable for the reasonable cost of attorneys' fees, court costs, expert witness fees, and other litigation expenses for the State to enforce the terms of this Contract.

Docusign Envelope ID: 40B7BFA4-E1BB-4360-9C9C-6FA33E97F12A

In the event of any suit or claim, the Parties shall give each other immediate notice and provide all necessary assistance to respond. The failure of the State to give notice shall only relieve the Contractor of its obligations under this Section to the extent that the Contractor can demonstrate actual prejudice arising from the failure to give notice. This Section shall not grant the Contractor, through its attorneys, the right to represent the State in any legal matter, as the right to represent the State is governed by Tenn. Code Ann. § 8-6-106.

D.20. HIPAA Compliance. The State and Contractor shall comply with obligations under the Health Insurance Portability and Accountability Act of 1996 ("HIPAA"), Health Information Technology for Economic and Clinical Health ("HITECH") Act and any other relevant laws and regulations regarding privacy (collectively the "Privacy Rules"). The obligations set forth in this Section shall survive the termination of this Contract.

a. Contractor warrants to the State that it is familiar with the requirements of the Privacy Rules, and will comply with all applicable requirements in the course of this Contract.

b. Contractor warrants that it will cooperate with the State, including cooperation and coordination with State privacy officials and other compliance officers required by the Privacy Rules, in the course of performance of the Contract so that both parties will be in compliance with the Privacy Rules.

c. The State and the Contractor will sign documents, including but not limited to business associate agreements, as required by the Privacy Rules and that are reasonably necessary to keep the State and Contractor in compliance with the Privacy Rules. This provision shall not apply if information received or delivered by the parties under this Contract is NOT "protected health information" as defined by the Privacy Rules, or if the Privacy Rules permit the parties to receive or deliver the information without entering into a business associate agreement or signing another document.

d. The Contractor will indemnify the State and hold it harmless for any violation by the Contractor or its subcontractors of the Privacy Rules. This includes the costs of responding to a breach of protected health information, the costs of responding to a government enforcement action related to the breach, and any fines, penalties, or damages paid by the State because of the violation.

D.21. Tennessee Consolidated Retirement System. Subject to statutory exceptions contained in Tenn. Code Ann. §§ 8-36-801, *et seq.*, the law governing the Tennessee Consolidated Retirement System ("TCRS"), provides that if a retired member of TCRS, or of any superseded system administered by TCRS, or of any local retirement fund established under Tenn. Code Ann. §§ 8-35-101, *et seq.*, accepts State employment, the member's retirement allowance is suspended during the period of the employment. Accordingly and notwithstanding any provision of this Contract to the contrary, the Contractor agrees that if it is later determined that the true nature of the working relationship between the Contractor and the State under this Contract is that of "employee/employer" and not that of an independent contractor, the Contractor, if a retired member of TCRS, may be required to repay to TCRS the amount of retirement benefits the Contractor received from TCRS during the Term.

D.22. Tennessee Department of Revenue Registration. The Contractor shall comply with all applicable registration requirements contained in Tenn. Code Ann. §§ 67-6-601 – 608. Compliance with applicable registration requirements is a material requirement of this Contract,

D.23. Debarment and Suspension. The Contractor certifies, to the best of its knowledge and belief, that it, its current and future principals, its current and future subcontractors and their principals:

a. are not presently debarred, suspended, proposed for debarment, declared ineligible, or voluntarily excluded from covered transactions by any federal or state department or agency;

Docusign Envelope ID: 40B7BFA4-E1BB-4360-9C9C-6FA33E97F12A

b. have not within a three (3) year period preceding this Contract been convicted of, or had a civil judgment rendered against them from commission of fraud, or a criminal offense in connection with obtaining, attempting to obtain, or performing a public (federal, state, or local) transaction or grant under a public transaction; violation of federal or state antitrust statutes or commission of embezzlement, theft, forgery, bribery, falsification, or destruction of records, making false statements, or receiving stolen property;

c. are not presently indicted or otherwise criminally or civilly charged by a government entity (federal, state, or local) with commission of any of the offenses detailed in section b. of this certification; and

d. have not within a three (3) year period preceding this Contract had one or more public transactions (federal, state, or local) terminated for cause or default.

The Contractor shall provide immediate written notice to the State if at any time it learns that there was an earlier failure to disclose information or that due to changed circumstances, its principals or the principals of its subcontractors are excluded, disqualified, or presently fall under any of the prohibitions of sections a-d.

D.24. Force Majeure. "Force Majeure Event" means fire, flood, earthquake, elements of nature or acts of God, wars, riots, civil disorders, rebellions or revolutions, acts of terrorism or any other similar cause beyond the reasonable control of the Party except to the extent that the non-performing Party is at fault in failing to prevent or causing the default or delay, and provided that the default or delay cannot reasonably be circumvented by the non-performing Party through the use of alternate sources, workaround plans or other means. A strike, lockout or labor dispute shall not excuse either Party from its obligations under this Contract. Except as set forth in this Section, any failure or delay by a Party in the performance of its obligations under this Contract arising from a Force Majeure Event is not a default under this Contract or grounds for termination. The non-performing Party will be excused from performing those obligations directly affected by the Force Majeure Event, and only for as long as the Force Majeure Event continues, provided that the Party continues to use diligent, good faith efforts to resume performance without delay. The occurrence of a Force Majeure Event affecting Contractor's representatives, suppliers, subcontractors, customers or business apart from this Contract is not a Force Majeure Event under this Contract. Contractor will promptly notify the State of any delay caused by a Force Majeure Event (to be confirmed in a written notice to the State within one (1) day of the inception of the delay) that a Force Majeure Event has occurred, and will describe in reasonable detail the nature of the Force Majeure Event. If any Force Majeure Event results in a delay in Contractor's performance longer than forty-eight (48) hours, the State may, upon notice to Contractor: (a) cease payment of the fees for the affected obligations until Contractor resumes performance of the affected obligations; or (b) immediately terminate this Contract or any purchase order, in whole or in part, without further payment except for fees then due and payable. Contractor will not increase its charges under this Contract or charge the State any fees other than those provided for in this Contract as the result of a Force Majeure Event.

D.25. State and Federal Compliance. The Contractor shall comply with all State and federal laws and regulations applicable to Contractor in the Contractor's performance of this Contract.

D.26. Governing Law. This Contract shall be governed by and construed in accordance with the laws of the State of Tennessee, without regard to its conflict or choice of law rules. The Tennessee Claims Commission or the state or federal courts in Tennessee shall be the venue for all claims, disputes, or disagreements arising under this Contract. The Contractor acknowledges and agrees that any rights, claims, or remedies against the State of Tennessee or its employees arising under this Contract shall be subject to and limited to those rights and remedies available under Tenn. Code Ann. §§ 9-8-101 - 408.

D.27. Entire Agreement. This Contract is complete and contains the entire understanding between the Parties relating to its subject matter, including all the terms and conditions of the Parties'

Docusign Envelope ID: 40B7BFA4-E1BB-4360-9C9C-6FA33E97F12A

agreement. This Contract supersedes any and all prior understandings, representations, negotiations, and agreements between the Parties, whether written or oral.

D.28. Severability. If any terms and conditions of this Contract are held to be invalid or unenforceable as a matter of law, the other terms and conditions of this Contract shall not be affected and shall remain in full force and effect. The terms and conditions of this Contract are severable.

D.29. Headings. Section headings of this Contract are for reference purposes only and shall not be construed as part of this Contract.

D.30. Incorporation of Additional Documents. Each of the following documents is included as a part of this Contract by reference. In the event of a discrepancy or ambiguity regarding the Contractor's duties, responsibilities, and performance under this Contract, these items shall govern in order of precedence below:

a. any amendment to this Contract, with the latter in time controlling over any earlier amendments;
b. this Contract with any attachments or exhibits (excluding the items listed at subsections c. through f., below), which includes:
    1. Attachment A – Definitions and Abbreviations;
    2. Attachment B – Service Level Agreements and Liquidated Damages;
    3. Attachment C – Procurement Library;
        a) TennCare Solution Implementation Lifecycle (SILC) Standard
        b) MSS -TennCare Solution Implementation Lifecycle RACI and Deliverables
        c) Cloud Security Questionnaire
        d) TennCare Privacy, Security and Confidentiality Training Policy (PRIV-013)
        e) TennCare Privacy Program Policy and Plan (PRIV-028)
        f) TennCare Records Retention Policy
        g) TennCare Records Disposition Authorization (RDA) List
        h) TennCare Data Policies & Standards
        i) TennCare Enterprise Architecture Framework Standard
        j) TennCare Project Management Plan Standard
        k) TennCare Test Management Standard
        l) TennCare IT Service Management Standard
        m) TennCare IT Service Management RACI
        n) TennCare Data Conversion Standard
        o) TennCare Security Policies
            1) TennCare Personnel Security Policy
            2) TennCare Access Control Policy
            3) TennCare Audit and Accountability Policy
            4) TennCare Configuration Management Policy
            5) TennCare Contingency Planning

Docusign Envelope ID: 40B7BFA4-E1BB-4360-9C9C-6FA33E97F12A

6) TennCare Identification and Authentication Policy
7) TennCare Incident Response Policy
8) TennCare Maintenance Policy
9) TennCare Media Protection Policy
10) TennCare Physical and Environmental Protection Policy
11) TennCare Planning Policy
12) TennCare Program Management Policy
13) TennCare Risk Assessment Policy
14) TennCare Security Assessment and Authorization Policy
15) TennCare Security Awareness and Training Policy
16) TennCare Security System and Information Integrity Policy
17) TennCare Security Systems and Communication Policy
18) TennCare System and Services Acquisition Policy

4. Attachment D – Contract Requirements Inventory;
5. Attachment E – Attestation Re: Personnel Use in Contract Performance;
6. Attachment F – HIPAA Business Associate Agreement; and
7. Attachment G – Cost Proposal.

c. any clarifications of or addenda to the Contractor's proposal seeking this Contract;
d. the State solicitation, as may be amended, requesting responses in competition for this Contract;
e. any technical specifications provided to proposers during the procurement process to award this Contract; and
f. the Contractor's response seeking this Contract.

D.31. Iran Divestment Act. The requirements of Tenn. Code Ann. § 12-12-101, *et seq.*, addressing contracting with persons as defined at Tenn. Code Ann. §12-12-103(5) that engage in investment activities in Iran, shall be a material provision of this Contract. The Contractor certifies, under penalty of perjury, that to the best of its knowledge and belief that it is not on the list created pursuant to Tenn. Code Ann. § 12-12-106.

D.32. Insurance. Contractor shall maintain insurance coverage as specified in this Section. The State reserves the right to amend or require additional insurance coverage, coverage amounts, and endorsements required under this Contract. Contractor's failure to maintain or submit evidence of insurance coverage, as required, is a material breach of this Contract. If Contractor loses insurance coverage, fails to renew coverage, or for any reason becomes uninsured during the Term, Contractor shall immediately notify the State. All insurance companies providing coverage must be: (a) acceptable to the State; (b) authorized by the Tennessee Department of Commerce and Insurance ("TDCI"); and (c) rated A- / VII or better by A.M. Best. All coverage must be on a primary basis and noncontributory with any other insurance or self-insurance carried by the State. Contractor agrees to name the State as an additional insured on any insurance policy with the exception of workers' compensation (employer liability) and professional liability (errors and omissions) insurance. All policies must contain an endorsement for a waiver of subrogation in favor of the State. Any deductible or self-insured retention ("SIR") over fifty thousand dollars ($50,000) must be approved by the State. The deductible or SIR and any premiums are the Contractor's sole responsibility. The Contractor agrees that the insurance requirements specified in this Section do not reduce any liability the Contractor has assumed under this Contract including any indemnification or hold harmless requirements.

Docusign Envelope ID: 40B7BFA4-E1BB-4360-9C9C-6FA33E97F12A

To achieve the required coverage amounts, a combination of an otherwise deficient specific policy and an umbrella policy with an aggregate meeting or exceeding the required coverage amounts is acceptable. For example: If the required policy limit under this Contract is for two million dollars ($2,000,000) in coverage, acceptable coverage would include a specific policy covering one million dollars ($1,000,000) combined with an umbrella policy for an additional one million dollars ($1,000,000). If the deficient underlying policy is for a coverage area without aggregate limits (generally Automobile Liability and Employers' Liability Accident), Contractor shall provide a copy of the umbrella insurance policy documents to ensure that no aggregate limit applies to the umbrella policy for that coverage area. In the event that an umbrella policy is being provided to achieve any required coverage amounts, the umbrella policy shall be accompanied by an endorsement at least as broad as the Insurance Services Office, Inc. (also known as "ISO") "Noncontributory—Other Insurance Condition" endorsement or shall be written on a policy form that addresses both the primary and noncontributory basis of the umbrella policy if the State is otherwise named as an additional insured.

Contractor shall provide the State a certificate of insurance ("COI") evidencing the coverages and amounts specified in this Section. The COI must be on a form approved by the TDCI (standard ACORD form preferred). The COI must list each insurer's National Association of Insurance Commissioners (NAIC) number and be signed by an authorized representative of the insurer. The COI must list the State of Tennessee – CPO Risk Manager, 312 Rosa L. Parks Ave., 3rd floor Central Procurement Office, Nashville, TN 37243 as the certificate holder. Contractor shall provide the COI ten (10) business days prior to the Effective Date and again thirty (30) calendar days before renewal or replacement of coverage. Contractor shall provide the State evidence that all subcontractors maintain the required insurance or that subcontractors are included under the Contractor's policy. At any time, the State may require Contractor to provide a valid COI. The Parties agree that failure to provide evidence of insurance coverage as required is a material breach of this Contract. If Contractor self-insures, then a COI will not be required to prove coverage. Instead Contractor shall provide a certificate of self-insurance or a letter, on Contractor's letterhead, detailing its coverage, policy amounts, and proof of funds to reasonably cover such expenses. The State reserves the right to require complete copies of all required insurance policies, including endorsements required by these specifications, at any time.

The State agrees that it shall give written notice to the Contractor as soon as practicable after the State becomes aware of any claim asserted or made against the State, but in no event later than thirty (30) calendar days after the State becomes aware of such claim. The failure of the State to give notice shall only relieve the Contractor of its obligations under this Section to the extent that the Contractor can demonstrate actual prejudice arising from the failure to give notice. This Section shall not grant the Contractor or its insurer, through its attorneys, the right to represent the State in any legal matter, as the right to represent the State is governed by Tenn. Code Ann. § 8-6-106.

The insurance obligations under this Contract shall be: (1)—all the insurance coverage and policy limits carried by the Contractor; or (2)—the minimum insurance coverage requirements and policy limits shown in this Contract; whichever is greater. Any insurance proceeds in excess of or broader than the minimum required coverage and minimum required policy limits, which are applicable to a given loss, shall be available to the State. No representation is made that the minimum insurance requirements of the Contract are sufficient to cover the obligations of the Contractor arising under this Contract. The Contractor shall obtain and maintain, at a minimum, the following insurance coverages and policy limits.

a. Commercial General Liability ("CGL") Insurance

    1) The Contractor shall maintain CGL, which shall be written on an ISO Form CG 00 01 occurrence form (or a substitute form providing equivalent coverage) and

Docusign Envelope ID: 40B7BFA4-E1BB-4360-9C9C-6FA33E97F12A

shall cover liability arising from property damage, premises and operations products and completed operations, bodily injury, personal and advertising injury, and liability assumed under an insured contract (including the tort liability of another assumed in a business contract).
The Contractor shall maintain single limits not less than one million dollars ($1,000,000) per occurrence. If a general aggregate limit applies, either the general aggregate limit shall apply separately to this policy or location of occurrence or the general aggregate limit shall be twice the required occurrence limit.

b. Workers' Compensation and Employer Liability Insurance

1) For Contractors statutorily required to carry workers' compensation and employer liability insurance, the Contractor shall maintain:

i. Workers' compensation in an amount not less than one million dollars ($1,000,000) including employer liability of one million dollars ($1,000,000) per accident for bodily injury by accident, one million dollars ($1,000,000) policy limit by disease, and one million dollars ($1,000,000) per employee for bodily injury by disease.

2) If the Contractor certifies that it is exempt from the requirements of Tenn. Code Ann. §§ 50-6-101 – 103, then the Contractor shall furnish written proof of such exemption for one or more of the following reasons:

i. The Contractor employs fewer than five (5) employees;

ii. The Contractor is a sole proprietor;

iii. The Contractor is in the construction business or trades with no employees;

iv. The Contractor is in the coal mining industry with no employees;

v. The Contractor is a state or local government; or

vi. The Contractor self-insures its workers' compensation and is in compliance with the TDCI rules and Tenn. Code Ann. § 50-6-405.

c. Automobile Liability Insurance

1) The Contractor shall maintain automobile liability insurance which shall cover liability arising out of any automobile (including owned, leased, hired, and non-owned automobiles).

2) The Contractor shall maintain bodily injury/property damage with a limit not less than one million dollars ($1,000,000) per occurrence or combined single limit.

d. Technology Professional Liability (Errors & Omissions)/Cyber Liability Insurance

1) The Contractor shall maintain technology professional liability (errors & omissions)/cyber liability insurance appropriate to the Contractor's profession in an amount not less than ten million dollars ($10,000,000) per occurrence or claim and ten million dollars ($10,000,000) annual aggregate, covering all acts, claims,

Docusign Envelope ID: 40B7BFA4-E1BB-4360-9C9C-6FA33E97F12A

errors, omissions, negligence, infringement of intellectual property (including copyright, patent and trade secret); network security and privacy risks, including but not limited to unauthorized access, failure of security, information theft, damage to destruction of or alteration of electronic information, breach of privacy perils, wrongful disclosure and release of private information, collection, or other negligence in the handling of confidential information, and including coverage for related regulatory fines, defenses, and penalties.

2) Such coverage shall include data breach response expenses, in an amount not less than ten million dollars ($10,000,000) and payable whether incurred by the State or Contractor, including but not limited to consumer notification, whether or not required by law, computer forensic investigations, public relations and crisis management firm fees, credit file or identity monitoring or remediation services and expenses in the performance of services for the State or on behalf of the State hereunder.

e. Crime Insurance

1) The Contractor shall maintain crime insurance, which shall be written on a "loss sustained form" or "loss discovered form" providing coverage for third party fidelity, including cyber theft and extortion. The policy must allow for reporting of circumstances or incidents that may give rise to future claims, include an extended reporting period of no less than two (2) years with respect to events which occurred but were not reported during the term of the policy, and not contain a condition requiring an arrest or conviction.

2) Any crime insurance policy shall have a limit not less than one million dollars ($1,000,000) per claim and one million dollars ($1,000,000) in the aggregate. Any crime insurance policy shall contain a Social Engineering Fraud Endorsement with a limit of not less than two hundred and fifty thousand dollars ($250,000). This insurance may be written on a claims-made basis, but in the event that coverage is cancelled or non-renewed, the Contractor shall purchase an extended reporting or "tail coverage" of at least two (2) years after the Term.

f. Professional Liability

i. Professional liability insurance shall be written on an occurrence basis or on a claims-made basis. If this coverage is written on a claims-made basis, then:
   i. The retroactive date must be shown, and must be on or before the earlier of the Effective Date of the Contract or the beginning of Contract work or provision of goods and services;
   ii. Insurance must be maintained and evidence of insurance must be provided for at least five (5) full years from the date of the final Contract payment; and
   iii. If coverage is canceled or non-renewed, and not replaced with another claims-made policy form with a retroactive date on or prior to the Contract Effective Date, the Contractor must purchase "extended reporting" or "tail coverage" for a minimum of five (5) full years from the date of the final Contract payment.

ii. Any professional liability insurance policy shall have a limit not less than one million dollars ($1,000,000) per claim and two million dollars ($2,000,000) in the aggregate.

iii. If the Contract involves the provision of services by medical professionals, a policy limit not less than three million ($3,000,000) per claim and three million dollars ($3,000,000) in the aggregate for medical malpractice insurance.

Docusign Envelope ID: 40B7BFA4-E1BB-4360-9C9C-6FA33E97F12A

D.33. Major Procurement Contract Sales and Use Tax. Pursuant to Tenn. Code Ann. § 4-39-102 and to the extent applicable, the Contractor and the Contractor's subcontractors shall remit sales and use taxes on the sales of goods or services that are made by the Contractor or the Contractor's subcontractors and that are subject to tax.

D.34. Confidentiality of Records. Strict standards of confidentiality of records and information shall be maintained in accordance with applicable state and federal law. All material and information, regardless of form, medium or method of communication, provided to the Contractor by the State or acquired by the Contractor on behalf of the State that is regarded as confidential under state or federal law shall be regarded as "Confidential Information." Nothing in this Section shall permit Contractor to disclose any Confidential Information, regardless of whether it has been disclosed or made available to the Contractor due to intentional or negligent actions or inactions of agents of the State or third parties. Confidential Information shall not be disclosed except as required or permitted under state or federal law. The Contractor shall only use Confidential Information for activities pursuant to and related to the performance of the Contract. Contractor shall take all necessary steps to safeguard the confidentiality of such material or information in conformance with applicable state and federal law.

The obligations set forth in this Section shall survive the termination of this Contract.

D.35. Equal Opportunity. The Contractor agrees as follows:

a. The Contractor will not discriminate against any employee or applicant for employment because of disability, race, color, religion, sex, sexual orientation, gender identity, or national origin. The Contractor will take affirmative action to ensure that applicants are employed, and that employees are treated during employment, without regard to their disability, race, color, religion, sex, sexual orientation, gender identity, or national origin. Such action shall include, but not be limited to the following:

(1) Employment, upgrading, demotion, or transfer, recruitment or recruitment advertising;

(2) Layoff or termination;

(3) Rates of pay or other forms of compensation; and

(4) Selection for training, including apprenticeship.

The Contractor agrees to post in conspicuous places, available to employees and applicants for employment, notices to be provided by the contracting officer setting forth the provisions of this nondiscrimination clause.

b. The Contractor will, in all solicitations or advertisements for employees placed by or on behalf of the Contractor, state that all qualified applicants will receive considerations for employment without regard to disability, race, color, religion, sex, sexual orientation, gender identity, or national origin.

c. If the State approves any subcontract, the subcontract shall include paragraphs (a) and (b) above.

d. In addition, to the extent applicable the Contractor agrees to comply with 41 C.F. R. § 60-1.4, as that section is amended from time to time during the term.

D.36. Boycott of Israel. The Contractor certifies that it is not currently engaged in, and covenants that it will not, for the duration of the Contract, engage in a Boycott of Israel, as that term is defined in Tenn. Code Ann. § 12-4-119.

D.37. Prohibited Contract Terms. The prohibited contract terms and conditions enumerated in Pub. Ch. 113, § 5, shall be a material provision of this Contract. The Contractor acknowledges, understands, and agrees that the inclusion of a term or condition prohibited by Pub. Ch. 113, § 5,

Docusign Envelope ID: 40B7BFA4-E1BB-4360-9C9C-6FA33E97F12A

shall be null and void and the Contract shall be enforceable as if the Contract did not contain such term or condition.

E. SPECIAL TERMS AND CONDITIONS:

E.1. Conflicting Terms and Conditions. Should any of these special terms and conditions conflict with any other terms and conditions of this Contract, the special terms and conditions shall be subordinate to the Contract's other terms and conditions.

E.2. Contractor Commitment to Diversity. The Contractor shall comply with and make reasonable business efforts to exceed the commitment to diversity represented by the Contractor's Response to RFP #31865-00641 and resulting in this Contract.

The Contractor shall assist the State in monitoring the Contractor's performance of this commitment by providing, as requested, a monthly report of participation in the performance of this Contract by small business enterprises and businesses owned by minorities, women, service-disabled veterans, and persons with disabilities. Such reports shall be provided to the State of Tennessee Governor's Office of Diversity Business Enterprise in the TN Diversity Software available online at: https://tn.diversitysoftware.com/FrontEnd/StartCertification.asp?TN=tn&XID=9810.

E.3. State Ownership of Goods. The State shall have ownership, right, title, and interest in all goods provided by Contractor under this Contract including full rights to use the goods and transfer title in the goods to any third parties.

E.4. Printing Authorization. The Contractor agrees that no publication coming within the jurisdiction of Tenn. Code Ann. §§ 12-7-101, et. seq. shall be printed pursuant to this Contract unless a printing authorization number has been obtained and affixed as required by Tenn. Code Ann. § 12-7-103 (d).

E.5. Additional lines, items, or options. At its sole discretion, the State may make written requests to the Contractor to add lines, items, or options that are needed and within the Scope but were not included in the original Contract. Such lines, items, or options will be added to the Contract through a Memorandum of Understanding ("MOU"), not an amendment.

a. After the Contractor receives a written request to add lines, items, or options, the Contractor shall have ten (10) business days to respond with a written proposal. The Contractor's written proposal shall include:

(1) The effect, if any, of adding the lines, items, or options on the other goods or services required under the Contract;

(2) Any pricing related to the new lines, items, or options;

(3) The expected effective date for the availability of the new lines, items, or options; and

(4) Any additional information requested by the State.

b. The State may negotiate the terms of the Contractor's proposal by requesting revisions to the proposal.

c. To indicate acceptance of a proposal, the State will sign it. The signed proposal shall constitute a MOU between the Parties, and the lines, items, or options shall be incorporated into the Contract as if set forth verbatim.

d. Only after a MOU has been executed shall the Contractor perform or deliver the new lines, items, or options.

E.6. Intellectual Property Indemnity. The Contractor agrees to indemnify and hold harmless the State of Tennessee as well as its officers, agents, and employees from and against any and all claims or suits which may be brought against the State concerning or arising out of any claim of an

Docusign Envelope ID: 40B7BFA4-E1BB-4360-9C9C-6FA33E97F12A

alleged patent, copyright, trade secret or other intellectual property infringement. In any such claim or action brought against the State, the Contractor shall satisfy and indemnify the State for the amount of any settlement or final judgment, and the Contractor shall be responsible for all legal or other fees or expenses incurred by the State arising from any such claim. The State shall give the Contractor notice of any such claim or suit, however, the failure of the State to give such notice shall only relieve Contractor of its obligations under this Section to the extent Contractor can demonstrate actual prejudice arising from the State's failure to give notice. This Section shall not grant the Contractor, through its attorneys, the right to represent the State of Tennessee in any legal matter, as provided in Tenn. Code Ann. § 8-6-106.

E.7. Software License Warranty. Contractor grants a license to the State to use all software provided under this Contract in the course of the State's business and purposes.

E.8. Software Support and Maintenance Warranty. Contractor shall provide to the State all software upgrades, modifications, bug fixes, or other improvements in its software that it makes generally available to its customers.

E.9. Extraneous Terms and Conditions. Contractor shall fill all orders submitted by the State under this Contract. No purchase order, invoice, or other documents associated with any sales, orders, or supply of any good or service under this Contract shall contain any terms or conditions other than as set forth in the Contract. Any such extraneous terms and conditions shall be void, invalid and unenforceable against the State. Any refusal by Contractor to supply any goods or services under this Contract conditioned upon the State submitting to any extraneous terms and conditions shall be a material breach of the Contract and constitute an act of bad faith by Contractor.

E.10. Transfer of Ownership of Custom Software Developed for the State.

a. Definitions.

1) "Contractor-Owned Software," shall mean commercially available software the rights to which are owned by Contractor, including but not limited to commercial "off-the-shelf" software which is not developed using State's money or resources.

2) "Custom-Developed Application Software," shall mean customized application software developed by Contractor solely for State under this Contract intended to function with the Contractor-Owned Software or any Work Product provided under this Contract.

3) "Rights Transfer Application Software," shall mean any pre-existing application software and documentation owned or supplied by Contractor or a third party necessary for the use, functioning, support, or maintenance of the Contractor-Owned Software, the Custom-Developed Application Software, Third Party Software, and any Work Product provided to State.

4) "Third-Party Software," shall mean software supplied by Contractor under this Contract or necessary for the functioning of any Work Product not owned by the State or the Contractor.

5) "Work Product," shall mean all deliverables such as software, software source code, documentation, planning, etc., that are created, designed, developed, or documented by the Contractor exclusively for the State under this Contract. Work Product shall include Rights Transfer Application Software.

b. Rights and Title to the Software

1) All right, title and interest in and to the Contractor-Owned Software shall at all times remain with Contractor, subject to any license or transfer of rights or ownership granted under this Contract. Contractor grants the State a non-exclusive license to the Contractor-Owned Software to be used solely with the Custom-Developed Application Software and the Work Product for the duration of this contract term.

Docusign Envelope ID: 40B7BFA4-E1BB-4360-9C9C-6FA33E97F12A

2) Contractor shall provide the source code in the Custom-Developed Application Software, Work Product and the Contractor-Owned Software, with all subsequent modifications, enhancements, bug-fixes or any other changes in the source code of the Work Product and the Contractor-Owned Software and all other code and documentation necessary for the Custom-Developed Application Software to be installed and function as intended and as set forth in this Contract, to the State.

3) Contractor may lease or sell the Custom-Developed Application Software to third parties with the written permission of the State, which permission may be conditioned on the State receiving royalties from such sales or licenses.

4) All right, title and interest in and to the Custom-Developed Application Software, and to modifications thereof made by State, including without limitation all copyrights, patents, trade secrets and other intellectual property and other proprietary rights embodied by and arising out of the Custom-Developed Application Software, shall belong to State. To the extent such rights do not automatically belong to State, Contractor hereby assigns, transfers, and conveys all right, title and interest in and to the Custom-Developed Application Software, including without limitation the copyrights, patents, trade secrets, and other intellectual property rights arising out of or embodied by the Custom-Developed Application Software. Contractor and its employees, agents, contractors or representatives shall execute any other documents that State or its counsel deem necessary or desirable to document this transfer or allow State to register its claims and rights to such intellectual property rights or enforce them against third parties.

5) All right, title and interest in and to the Third-Party Software shall at all times remain with the third party, subject to any license or other rights granted to the State under this Contract.

c. The Contractor may use for its own purposes the general knowledge, skills, experience, ideas, concepts, know-how, and techniques obtained and used during the course of performing under this Contract. The Contractor may develop for itself, or for others, materials which are similar to or competitive with those that are produced under this Contract.

d. Notwithstanding anything to the contrary in this Section, the State shall have all ownership rights in software or modifications thereof and associated documentation that is designed, developed, installed, or improved hereunder with Federal Financial Participation under 45 C.F.R. 95.617 and 45 C.F.R. 92.34, and the Federal government reserves a royalty-free, nonexclusive, and irrevocable license to reproduce, publish, or otherwise use and to authorize others to use for Federal Government purposes, such software, modification, and documentation.

E.11. Contractor Hosted Services Confidential Data, Audit, and Other Requirements

a. "Confidential State Data" is defined as data deemed confidential by State or Federal statute or regulation. The Contractor shall protect Confidential State Data as follows:

(1) The Contractor shall ensure that all Confidential State Data is housed in the continental United States, inclusive of backup data.

(2) The Contractor shall encrypt Confidential State Data at rest and in transit using the current version of Federal Information Processing Standard ("FIPS") 140-2 or 140-3 (current applicable version) validated encryption technologies. The State shall control all access to encryption keys. The Contractor shall provide installation and maintenance support at no cost to the State.

Docusign Envelope ID: 40B7BFA4-E1BB-4360-9C9C-6FA33E97F12A

(3) The Contractor and the Contractor's processing environment containing Confidential State Data shall either (1) be in accordance with at least one of the following security standards: (i) International Standards Organization ("ISO") 27001; (ii) Federal Risk and Authorization Management Program ("FedRAMP"); or (2) be subject to an annual engagement by a CPA firm in accordance with the standards of the American Institute of Certified Public Accountants ("AICPA") for a System and Organization Controls for service organizations ("SOC") Type II audit. The State shall approve the SOC audit control objectives. The Contractor shall provide proof of current ISO certification or FedRAMP authorization for the Contractor and Subcontractor(s), or provide the State with the Contractor's and Subcontractor's annual SOC Type II audit report within 30 days from when the CPA firm provides the audit report to the Contractor or Subcontractor. The Contractor shall submit corrective action plans to the State for any issues included in the audit report within 30 days after the CPA firm provides the audit report to the Contractor or Subcontractor.

If the scope of the most recent SOC audit report does not include all of the current State fiscal year, upon request from the State, the Contractor must provide to the State a letter from the Contractor or Subcontractor stating whether the Contractor or Subcontractor made any material changes to their control environment since the prior audit and, if so, whether the changes, in the opinion of the Contractor or Subcontractor, would negatively affect the auditor's opinion in the most recent audit report.

No additional funding shall be allocated for these certifications, authorizations, or audits as these are included in the Maximum Liability of this Contract.

(4) The Contractor must annually perform Penetration Tests and Vulnerability Assessments against its Processing Environment. "Processing Environment" shall mean the combination of software and hardware on which the Application runs. "Application" shall mean the computer code that supports and accomplishes the State's requirements as set forth in this Contract. "Penetration Tests" shall be in the form of attacks on the Contractor's computer system, with the purpose of discovering security weaknesses which have the potential to gain access to the Processing Environment's features and data. The "Vulnerability Assessment" shall be designed and executed to define, identify, and classify the security holes (vulnerabilities) in the Processing Environment. The Contractor shall allow the State, at its option, to perform Penetration Tests and Vulnerability Assessments on the Processing Environment.

(5) Upon State request, the Contractor shall provide a copy of all Confidential State Data it holds. The Contractor shall provide such data on media and in a format determined by the State

(6) Upon termination of this Contract and in consultation with the State, the Contractor shall destroy all Confidential State Data it holds (including any copies such as backups) in accordance with the current version of National Institute of Standards and Technology ("NIST") Special Publication 800-88. The Contractor shall provide a written confirmation of destruction to the State within ten (10) business days after destruction.

(7) All State data must remain in the United States, regardless of whether the data is processed, stored, in-transit, or at rest.

i. Access to State data shall be limited to US-based (onshore) resources only.

Docusign Envelope ID: 40B7BFA4-E1BB-4360-9C9C-6FA33E97F12A

ii. Configuration or development of software and code is permitted outside of the United States. However, software applications designed, developed, manufactured, or supplied by persons owned or controlled by, or subject to the jurisdiction or direction of, a foreign adversary, which the U.S. Secretary of Commerce acting pursuant to 15 CFR 7has defined to include the People's Republic of China, among others are prohibited.

iii. Any testing of code outside of the United States must use fake data. A copy of production data may not be transmitted or used outside the United States.

b. Minimum Requirements

(1) The Contractor and all data centers used by the Contractor to host State data, including those of all Subcontractors, must comply with the State's Enterprise Information Security Policies as amended periodically. The State's Enterprise Information Security Policies document is found at the following URL: https://www.tn.gov/finance/strategic-technology-solutions/strategic-technology-solutions/sts-security-policies.html.

(2) The Contractor agrees to maintain the Application so that it will run on a current or N-1, manufacturer-supported Operating System. "Operating System" shall mean the software that supports a computer's basic functions, such as scheduling tasks, executing applications, and controlling peripherals.

(3) If the Application requires middleware or database software, Contractor shall maintain middleware and database software versions that are at all times fully compatible with current versions and that are reverse compatible with N-1 versions of the Operating System and Application to ensure that security vulnerabilities are not introduced.

c. Comptroller Audit Requirements

Upon reasonable notice and at any reasonable time, the Contractor and Subcontractor(s) agree to allow the State, the Comptroller of the Treasury, or their duly appointed representatives to perform information technology control audits of the Contractor and all Subcontractors used by the Contractor. Contractor will maintain and cause its Subcontractors to maintain a complete audit trail of all transactions and activities in connection with this Contract. Contractor will provide to the State, the Comptroller of the Treasury, or their duly appointed representatives access to Contractor and Subcontractor(s) personnel for the purpose of performing the information technology control audit.

The information technology control audit may include a review of general controls and application controls. General controls are the policies and procedures that apply to all or a large segment of the Contractor's or Subcontractor's information systems and applications and include controls over security management, access controls, configuration management, segregation of duties, and contingency planning. Application controls are directly related to the application and help ensure that transactions are complete, accurate, valid, confidential, and available. The audit shall include the Contractor's and Subcontractor's compliance with the State's Enterprise Information Security Policies and all applicable requirements, laws, regulations or policies.

Docusign Envelope ID: 40B7BFA4-E1BB-4360-9C9C-6FA33E97F12A

The audit may include interviews with technical and management personnel, physical inspection of controls, and review of paper or electronic documentation.

For any audit issues identified, the Contractor and Subcontractor(s) shall provide a corrective action plan to the State within 30 days from the Contractor or Subcontractor receiving the audit report.

Each party shall bear its own expenses incurred while conducting the information technology controls audit.

d. Business Continuity Requirements. The Contractor shall maintain set(s) of documents, instructions, and procedures which enable the Contractor to respond to accidents, disasters, emergencies, or threats without any stoppage or hindrance in its key operations ("Business Continuity Requirements"). Business Continuity Requirements shall include:

(1) "Disaster Recovery Capabilities" refer to the actions the Contractor takes to meet the Recovery Point and Recovery Time Objectives defined below. Disaster Recovery Capabilities shall meet the following objectives:

i. Recovery Point Objective ("RPO"). The RPO is defined as the maximum targeted period in which data might be lost from an IT service due to a major incident: twenty-four (24) hours.

ii. Recovery Time Objective ("RTO"). The RTO is defined as the targeted duration of time and a service level within which a business process must be restored after a disaster (or disruption) in order to avoid unacceptable consequences associated with a break in business continuity: two (2) hours.

(2) The Contractor and the Subcontractor(s) shall perform at least one Disaster Recovery Test every three hundred sixty-five (365) days. A "Disaster Recovery Test" shall mean the process of verifying the success of the restoration procedures that are executed after a critical IT failure or disruption occurs. The Disaster Recovery Test shall use actual State Data Sets that mirror production data, and success shall be defined as the Contractor verifying that the Contractor can meet the State's RPO and RTO requirements. A "Data Set" is defined as a collection of related sets of information that is composed of separate elements but can be manipulated as a unit by a computer. The Contractor shall provide written confirmation to the State after each Disaster Recovery Test that its Disaster Recovery Capabilities meet the RPO and RTO requirements.

E.12. State Furnished Property. The Contractor shall be responsible for the correct use, maintenance, and protection of all articles of nonexpendable, tangible personal property furnished by the State for the Contractor's use under this Contract. Upon termination of this Contract, all property furnished by the State shall be returned to the State in the same condition as when received, less reasonable wear and tear. Should the property be destroyed, lost, or stolen, the Contractor shall be responsible to the State for the fair market value of the property at the time of loss.

E.13. Work Papers Subject to Review. The Contractor shall make all audit, accounting, or financial analysis work papers, notes, and other documentation available for review by the Comptroller of the Treasury or his representatives, upon request, during normal working hours either while the analysis is in progress or subsequent to the completion of this Contract.

E.14. Prohibited Advertising or Marketing. The Contractor shall not suggest or imply in advertising or marketing materials that Contractor's goods or services are endorsed by the State. The

Docusign Envelope ID: 40B7BFA4-E1BB-4360-9C9C-6FA33E97F12A

restrictions on Contractor advertising or marketing materials under this Section shall survive the termination of this Contract.

E.15. Lobbying. The Contractor certifies, to the best of its knowledge and belief, that:

a. No federally appropriated funds have been paid or will be paid, by or on behalf of the Contractor, to any person for influencing or attempting to influence an officer or employee of an agency, a member of Congress, an officer or employee of Congress, or an employee of a member of Congress in connection with the awarding of any federal contract, the making of any federal grant, the making of any federal loan, the entering into of any cooperative agreement, and the extension, continuation, renewal, amendment, or modification of any federal contract, grant, loan, or cooperative agreement.

b. If any funds other than federally appropriated funds have been paid or will be paid to any person for influencing or attempting to influence an officer or employee of any agency, a member of Congress, an officer or employee of Congress, or an employee of a member of Congress in connection with any contract, grant, loan, or cooperative agreement, the Contractor shall complete and submit Standard Form-LLL, "Disclosure Form to Report Lobbying,'' in accordance with its instructions.

c. The Contractor shall require that the language of this certification be included in the award documents for all sub-awards at all tiers (including subcontracts, sub-grants, and contracts under grants, loans, and cooperative agreements) and that all subrecipients shall certify and disclose accordingly.

d. This certification is a material representation of fact upon which reliance was placed when this transaction was made or entered into and is a prerequisite for making or entering into this transaction imposed by 31 USC § 1352.

E.16. Liquidated Damages. In the event of a Contract performance or compliance failure by the Contractor, the State may, but is not obligated to address such Contract performance failure and/or assess damages ("Liquidated Damages") in accordance with Attachment B, Service Level Agreement and Liquidated Damages of the Contract. The State shall notify the Contractor of any amounts to be assessed as Liquidated Damages via the Control Memorandum process specified in Contract Section A.12.6. The Parties agree that due to the complicated nature of the Contractor's obligations under this Contract it would be difficult to specifically designate a monetary amount for a Contract performance or compliance failure, as these amounts are likely to be uncertain and not easily proven. Contractor has carefully reviewed the Liquidated Damages contained in Contract Attachment B, Service Level Agreements and Liquidated Damages and agrees that these amounts represent a reasonable relationship between the amount and what might reasonably be expected in the event of a Contract performance or compliance failure, are reasonable estimates of the damages that would occur from a Contract performance or compliance failure, and are not punitive. The Parties agree that although the Liquidated Damages represent the reasonable estimate of the damages and injuries sustained by the State due to the Contract performance or compliance failure, they do not include any injury or damage sustained by a third party. The Contractor agrees that the Liquidated Damages are in addition to any amounts Contractor may owe the State pursuant to the indemnity provision or any other sections of this Contract.

The State is not obligated to assess Liquidated Damages as a result of a Contract performance or compliance failure before availing itself of any other remedy. In the event of multiple Contract performance or compliance failures, the Parties recognize that the cumulative effect of these Contract performance failures may exceed the compensation provided by Liquidated Damages. The State may choose to avail itself of any other remedy available under this Contract or at law or equity. The Parties further recognize that the State may not obtain both Liquidated Damages and Actual Damages for the same occurrence of a Contract performance failure.

Docusign Envelope ID: 40B7BFA4-E1BB-4360-9C9C-6FA33E97F12A

Without regard to whether the State has imposed Liquidated Damages or pursued any other remedy due to any action or inaction by the Contractor, the State may impose a corrective action plan or similar measure through a Control Memorandum. Such measure is neither punitive nor related to any damages the State might suffer.

E.17. Partial Takeover of Contract**.** The State may, at its convenience and without cause, exercise a partial takeover of any service that the Contractor is obligated to perform under this Contract, including any service which is the subject of a subcontract between Contractor and a third party (a "Partial Takeover"). A Partial Takeover of this Contract by the State shall not be deemed a breach of contract. The Contractor shall be given at least thirty (30) days prior written notice of a Partial Takeover. The notice shall specify the areas of service the State will assume and the date the State will be assuming. The State's exercise of a Partial Takeover shall not alter the Contractor's other duties and responsibilities under this Contract. The State reserves the right to withhold from the Contractor any amounts the Contractor would have been paid but for the State's exercise of a Partial Takeover. The amounts shall be withheld effective as of the date the State exercises its right to a Partial Takeover. The State's exercise of its right to a Partial Takeover of this Contract shall not entitle the Contractor to any actual, general, special, incidental, consequential, or any other damages irrespective of any description or amount.

E.18. Unencumbered Personnel**.** The Contractor shall not restrict its employees, agents, subcontractors or principals who perform services for the State under this Contract from performing the same or similar services for the State after the termination of this Contract, either as a State employee, an independent contractor, or an employee, agent, subcontractor or principal of another contractor with the State.

E.19. Personally Identifiable Information**.** While performing its obligations under this Contract, Contractor may have access to Personally Identifiable Information held by the State ("PII"). For the purposes of this Contract, "PII" includes "Nonpublic Personal Information" as that term is defined in Title V of the Gramm-Leach-Bliley Act of 1999 or any successor federal statute, and the rules and regulations thereunder, all as may be amended or supplemented from time to time ("GLBA") and personally identifiable information and other data protected under any other applicable laws, rule or regulation of any jurisdiction relating to disclosure or use of personal information ("Privacy Laws"). Contractor agrees it shall not do or omit to do anything which would cause the State to be in breach of any Privacy Laws. Contractor shall, and shall cause its employees, agents and representatives to: (i) keep PII confidential and may use and disclose PII only as necessary to carry out those specific aspects of the purpose for which the PII was disclosed to Contractor and in accordance with this Contract, GLBA and Privacy Laws; and (ii) implement and maintain appropriate technical and organizational measures regarding information security to: (A) ensure the security and confidentiality of PII; (B) protect against any threats or hazards to the security or integrity of PII; and (C) prevent unauthorized access to or use of PII. Contractor shall immediately notify State: (1) of any disclosure or use of any PII by Contractor or any of its employees, agents and representatives in breach of this Contract; and (2) of any disclosure of any PII to Contractor or its employees, agents and representatives where the purpose of such disclosure is not known to Contractor or its employees, agents and representatives. The State reserves the right to review Contractor's policies and procedures used to maintain the security and confidentiality of PII and Contractor shall, and cause its employees, agents and representatives to, comply with all reasonable requests or directions from the State to enable the State to verify and/or procure that Contractor is in full compliance with its obligations under this Contract in relation to PII. Upon termination or expiration of the Contract or at the State's direction at any time in its sole discretion, whichever is earlier, Contractor shall immediately return to the State any and all PII which it has received under this Contract and shall destroy all records of such PII.

The Contractor shall report to the State any instances of unauthorized access to or potential disclosure of PII in the custody or control of Contractor ("Unauthorized Disclosure") that come to the Contractor's attention. Any such report shall be made by the Contractor within forty-eight (48) hours after the Unauthorized Disclosure has come to the attention of the Contractor. Contractor

Docusign Envelope ID: 40B7BFA4-E1BB-4360-9C9C-6FA33E97F12A

shall take all necessary measures to halt any further Unauthorized Disclosures. The Contractor, at the sole discretion of the State, shall provide no cost credit monitoring services for individuals whose PII was affected by the Unauthorized Disclosure. The Contractor shall bear the cost of notification to all individuals affected by the Unauthorized Disclosure, including individual letters and public notice. The remedies set forth in this Section are not exclusive and are in addition to any claims or remedies available to this State under this Contract or otherwise available at law. The obligations set forth in this Section shall survive the termination of this Contract.

E.20. Federal Funding Accountability and Transparency Act (FFATA). This Contract requires the Contractor to provide supplies or services that are funded in whole or in part by federal funds that are subject to FFATA. The Contractor is responsible for ensuring that all applicable requirements, including but not limited to those set forth herein, of FFATA are met and that the Contractor provides information to the State as required.

The Contractor shall comply with the following:

a) Reporting of Total Compensation of the Contractor's Executives.

1) The Contractor shall report the names and total compensation of each of its five most highly compensated executives for the Contractor's preceding completed fiscal year, if in the Contractor's preceding fiscal year it received:

i) 80 percent or more of the Contractor's annual gross revenues from federal procurement contracts and federal financial assistance subject to the Transparency Act, as defined at 2 CFR 170.320 (and subawards); and

ii) $25,000,000 or more in annual gross revenues from federal procurement contracts (and subcontracts), and federal financial assistance subject to the Transparency Act (and subawards); and

iii) The public does not have access to information about the compensation of the executives through periodic reports filed under section 13(a) or 15(d) of the Securities Exchange Act of 1934 (15 USC 78m(a), 78o(d)) or section 6104 of the Internal Revenue Code of 1986. (To determine if the public has access to the compensation information, see the U.S. Security and Exchange Commission total compensation filings at http://www.sec.gov/answers/execomp.htm).

As defined in 2 C.F.R. § 170.315, "Executive" means officers, managing partners, or any other employees in management positions.

2) Total compensation means the cash and noncash dollar value earned by the executive during the Contractor's preceding fiscal year and includes the following (for more information see 17 C.F.R. § 229.402l(2)):

i) Salary and bonus.

ii) Awards of stock, stock options, and stock appreciation rights. Use the dollar amount recognized for financial statement reporting purposes with respect to the fiscal year in accordance with the Statement of Financial Accounting Standards No. 123 (Revised 2004) (FAS 123R), Shared Based Payments.

iii) Earnings for services under non-equity incentive plans. This does not include group life, health, hospitalization or medical reimbursement plans that do not discriminate in favor of executives, and are available generally to all salaried employees.

iv) Change in pension value. This is the change in present value of defined benefit and actuarial pension plans.

v) Above-market earnings on deferred compensation which is not tax qualified.

Docusign Envelope ID: 40B7BFA4-E1BB-4360-9C9C-6FA33E97F12A

vi) Other compensation, if the aggregate value of all such other compensation (e.g. severance, termination payments, value of life insurance paid on behalf of the employee, perquisites or property) for the executive exceeds $10,000.

b) The Contractor must report executive total compensation described above to the State by the end of the month during which this Contract is awarded.

a. If this Contract is amended to extend the Term, the Contractor must submit an executive total compensation report to the State by the end of the month in which the term extension becomes effective.

b. The Contractor will obtain a Data Universal Numbering System (DUNS) number and maintain its DUNS number for the term of this Contract. More information about obtaining a DUNS Number can be found at: http://fedgov.dnb.com/webform/

The Contractor's failure to comply with the above requirements is a material breach of this Contract for which the State may terminate this Contract for cause. The State will not be obligated to pay any outstanding invoice received from the Contractor unless and until the Contractor is in full compliance with the above requirements.

E.21. Drug-Free Workplace. The Contractor shall provide a drug-free workplace pursuant to the Drug-Free Workplace Act of 1988, Title 41 U.S.C. §§ 701, *et seq.*, and the regulations in Title 41 U.S.C.A. §§ 8101 through 8106.

E.22. Survival. The terms, provisions, representations, and warranties contained in this Contract which by their sense and context are intended to survive the performance and termination of this Contract, shall so survive the completion of performance and termination of this Contract.

E.23. Applicable Legal Authority. The Contractor agrees to comply with all applicable legal authority, including federal and State laws, rules, regulations, policies, sub-regulatory guidance, the State Medicaid Manual, executive orders, TennCare waivers, and all current, modified or future Court decrees, orders or judgments applicable to the State's TennCare program. Such compliance shall be performed at no additional cost to the State.

E.24. Business Associate**.** As the Contractor will provide services to TennCare pursuant to which the Contractor will have access to, receive from, create, or receive on behalf of TennCare Protected Health Information, or Contractor will have access to, create, receive, maintain or transmit on behalf of TennCare Electronic Protected Health Information (as those terms are defined under HIPAA and HITECH), Contractor hereby acknowledges its designation as a business associate under HIPAA and agrees to comply with all applicable HIPAA regulations and any further responsibilities set forth in the Business Associate Agreement (See Attachment F) between the Parties.

E.25. Notification of Breach and Notification of Suspected Breach**.** The Contractor shall notify TennCare's Privacy Office immediately upon becoming aware of — and in no case later than forty-eight (48) hours after discovery of — any incident, either confirmed or suspected, that represents or may represent unauthorized access, use or disclosure of encrypted or unencrypted computerized data that materially compromises the security, confidentiality, or integrity of enrollee PHI maintained or held by the Contractor, including any unauthorized acquisition of enrollee PHI by an employee or otherwise Authorized User of the Contractor's system. This includes, but is not limited to, loss or suspected loss of remote computing or telework devices such as laptops, Personal Digital Assistants (PDAs), Blackberrys or other Smartphones, Universal Serial Bus (USB) drives, thumb drives, flash drives, Compact Discs (CD) , and/or hard disks.

E.26. Transmission of Contract Deliverables. All information or data that is necessary for one or more deliverable set forth in this Contract shall be transmitted between TennCare and Contractor via the data transfer method specified in advance by TennCare. This may include, but shall not be limited to, transfer through TennCare Secure File Transfer Protocol (SFTP) system. Failure by the Contractor to transmit information or data that is necessary for a deliverable in the manner

Docusign Envelope ID: 40B7BFA4-E1BB-4360-9C9C-6FA33E97F12A

specified by TennCare, may, at the option of TennCare, result in liquidated damages as set forth in Contract Attachment B – Service Level Agreements and Liquidated Damages.

E.27. Social Security Administration (SSA) Required Provisions for Data Security.

a. Definitions.

1. "SSA-supplied data" or "data" as used in this section means an individual's personally identifiable information (e.g., name, social security number, income), supplied by the Social Security Administration to TennCare to determine entitlement or eligibility for federally-funded programs pursuant to a Computer Matching and Privacy Protection Act Agreement and Information Exchange Agreement between SSA and the State of Tennessee.

b. The Contractor shall comply with limitations on use, treatment, and safeguarding of data under the Privacy Act of 1974 (5 U.S.C. 552a), as amended by the Computer Matching and Privacy Protection Act of 1988, related Office of Management and Budget guidelines, the Federal Information Security Management Act of 2002 (44 U.S.C. §3541, *et seq*.), and related National Institute of Standards and Technology guidelines, which provide the requirements that the SSA stipulates that the Contractor must follow with regard to use, treatment, and safeguarding data in the event data is exchanged with a federal information system. In addition, the Contractor shall have in place administrative, physical, and technical safeguards for data. The Contractor shall also comply with Section 1106(a) of the Act (42 U.S.C. 1306) and the regulations promulgated pursuant to that section (20 C.F.R. Part 401).

c. The Contractor shall specify in its agreements with any agent or subcontractor that will have access to data that such agent or subcontractor agrees to be bound by the same restrictions, terms and conditions that apply to the Contractor pursuant to this Section.

d. The Contractor shall not duplicate in a separate file or disseminate, without prior written permission from TennCare, the data governed by the Contract for any purpose other than that set forth in this Contract for the administration of the TennCare program. Should the Contractor propose a redisclosure of said data, the Contractor must specify in writing to TennCare the data the Contractor proposes to redisclose, to whom, and the reasons that justify the redisclosure. TennCare will not give permission for such redisclosure unless the redisclosure is required by law or essential to the administration of the TennCare program.

e. The Contractor agrees to abide by all relevant federal laws, restrictions on access, use, and disclosure, and security requirements in this Contract.

f. The Contractor shall maintain a current list of the employees of such contractor with access to SSA data and provide such lists to TennCare upon request and at any time there are changes.

g. The Contractor shall restrict access to the data obtained from TennCare to only those authorized employees who need such data to perform their official duties in connection with purposes identified in this Contract. The Contractor shall not further duplicate, disseminate, or disclose such data without obtaining TennCare's prior written approval.

h. The Contractor shall ensure that its employees:

1. Properly safeguard SSA-supplied data furnished by TennCare under this Contract from loss, theft, or inadvertent disclosure;
2. Receive regular, relevant, and sufficient SSA data-related training, including use, access, and disclosure safeguards and information regarding penalties for misuse of information;
3. Understand and acknowledge that they are responsible for safeguarding this information at all times, regardless of whether or not the Contractor employee is at his or her regular duty station;

Docusign Envelope ID: 40B7BFA4-E1BB-4360-9C9C-6FA33E97F12A

4. Ensure that laptops and other electronic devices/ media containing SSA-supplied data are encrypted and/or password-protected;
5. Send emails containing SSA-supplied data only if the information is encrypted or if the transmittal is secure; and,
6. Limit disclosure of the information and details relating to a SSA-supplied data loss only to those with a need to know.

i. Contractor employees who access, use, or disclose TennCare or TennCare SSA-supplied data in a manner or purpose not authorized by this Contract may be subject to civil and criminal sanctions pursuant to applicable federal statutes.

j. Loss or Suspected Loss of Data - If an employee of the Contractor becomes aware of suspected or actual loss of SSA-supplied data, the Contractor must notify TennCare immediately upon becoming aware to report the actual or suspected loss. The Contractor must provide TennCare with timely updates as any additional information about the loss of SSA-supplied data becomes available. If the Contractor experiences a loss or breach of said data, TennCare will determine whether or not notice to individuals whose data has been lost or breached shall be provided and the Contractor shall bear any costs associated with the notice or any mitigation.

k. TennCare may immediately and unilaterally suspend the data flow under this Contract, or terminate this Contract, if TennCare, in its sole discretion, determines that the Contractor has: (1) made an unauthorized use or disclosure of TennCare SSA-supplied data; or (2) otherwise violated or failed to follow the terms and conditions of this Contract.

E.28. Medicaid and CHIP. The Contractor must provide safeguards that restrict the use or disclosure of information concerning Medicaid and Children's Health Insurance Plan (CHIP) applicants and beneficiaries to purposes directly connected with the administration of the plan.

a. Purposes directly related to the administration of Medicaid and CHIP include:

1. Establishing eligibility;

2. Determining the amount of medical assistance;

3. Providing services for beneficiaries; and,

4. Conducting or assisting an investigation, prosecution, or civil or criminal proceeding related to Medicaid or CHIP administration.

b. The Contractor must have adequate safeguards to assure that:

1. Information is made available only to the extent necessary to assist in the valid administrative purposes of those receiving said information, and

2. Information received under the Internal Revenue Code (Title 26 of the United States Code (USC)) is exchanged only with parties authorized to receive that information under that section of the United States Code; and, the information is adequately stored and processed so that it is protected against unauthorized disclosure for other purposes.

c. The Contractor must have criteria that govern the types of information about applicants and beneficiaries that are safeguarded. This information must include, at minimum, the following:

1. Names and addresses;

Docusign Envelope ID: 40B7BFA4-E1BB-4360-9C9C-6FA33E97F12A

2. Medical services provided;
3. Social and economic conditions or circumstances;
4. Contractor evaluation of personal information;
5. Medical data, including diagnosis and past history of disease or disability;
6. Any information received for verifying income eligibility and amount of medical assistance payments, including income information received from the Social Security Administration (SSA) or the Internal Revenue Service (IRS);
7. Income information received from SSA or the IRS must be safeguarded according to Medicaid and CHIP requirements;
8. Any information received in connection with the identification of legally liable third-party resources; and,
9. Social Security Numbers.

d. The Contractor must have criteria approved by TennCare specifying:

1. Conditions for release and use of information about applicants and beneficiaries;
2. Access to information concerning applicants or beneficiaries must be restricted to Contractor representatives or other individuals who are subject to standards of confidentiality that are comparable to those of TennCare;
3. The Contractor shall not publish names of applicants or beneficiaries;
4. The Contractor shall obtain permission from a family or individual, whenever possible, before responding to a request for information from an outside source, unless the information is to be used to verify income, eligibility and the amount of medical assistance payment to an authorized individual or entity, or if, because of an emergency situation, time does not permit obtaining consent before release, the Contractor shall notify TennCare, the family, or individual immediately after supplying the information.
5. The Contractor's policies must apply to all requests for information from outside sources, including governmental bodies, the courts, or law enforcement officials.
6. The Contractor shall notify TennCare of any requests for information on applicants or beneficiaries by other governmental bodies, the courts or law enforcement officials ten (10) days prior to releasing the requested information.
7. If a court issues a subpoena for a case record or for any Contractor representative to testify concerning an applicant or beneficiary, the Contractor must notify TennCare at least ten (10) days prior to the required production date so TennCare may inform the court of the applicable statutory provisions, policies, and regulations restricting disclosure of information.
8. The Contractor shall not request or release information to other parties to verify income, eligibility, and the amount of assistance under Medicaid or CHIP prior to express approval from TennCare.

E.29. Employees Excluded from Medicare, Medicaid or CHIP. The Contractor does hereby attest, certify, warrant, and assure that the Contractor shall not knowingly employ, in the performance of this Contract, employees who have been excluded from participation in the Medicare, Medicaid, and/or CHIP programs pursuant to the Social Security Act, Section 1128 (Exclusion of Certain Individuals and Entities from Participation in Medicare and State Health Care Programs).

Docusign Envelope ID: 40B7BFA4-E1BB-4360-9C9C-6FA33E97F12A

E.30. Offer of Gratuities. By signing this Contract, the Contractor signifies that no member of or a delegate of Congress, nor any elected or appointed official or employee of the State of Tennessee, the federal General Accounting Office, federal Department of Health and Human Services, the CMS, or any other state or federal agency has or will benefit financially or materially from this Contract. This Contract may be terminated by TennCare as provided in Section D.6, if it is determined that gratuities of any kind were offered to or received by any of the aforementioned officials or employees from the Contractor, its agent, or employees.

E.31. Internal Revenue Service (IRS) Safeguarding Of Return Information:

a. PERFORMANCE

In performance of this Contract, the Contractor shall comply with, and assume responsibility for its officers' and employees' compliance with, the requirements outlined in Contract Section E.#. IRS Safeguard of Return Information. All cited regulations, statutes, publications, or IRS authority cited or referenced apply as they are in effect, or as subsequently amended or revised after the Effective Date of the Contract or any Amendment.

1) Contract Section E.31. IRS Safeguard of Return Information shall only apply if Contractor receives or delivers information under this Contract that is or includes "federal tax returns" or "federal return information" as defined by IRS Publication 1075 and IRC 6103.

2) All work will be performed under the supervision of the Contractor. The Contractor and Contractor's officers or employees to be authorized access to FTI must meet background check requirements defined in IRS Publication 1075. The Contractor will maintain a list of officers or employees authorized access to FTI. Such list will be provided to TennCare and, upon request, to the IRS.

3) FTI in hardcopy or electronic format shall be used only for the purpose of carrying out the provisions of this Contract. FTI in any format shall be treated as confidential and shall not be divulged or made known in any manner to any person except as may be necessary in the performance of this Contract. Inspection or disclosure of FTI to anyone other than the Contractor or the Contractor's officers or employees authorized is prohibited.

4) FTI will be accounted for upon receipt and properly stored before, during, and after processing. In addition, any related output and products require the same level of protection as required for the source material.

5) The Contractor will certify that FTI processed during the performance of this Contract will be completely purged from all physical and electronic data storage with no output to be retained by the Contractor at the time the work is completed. If immediate purging of physical and electronic data storage is not possible, the Contractor will certify that any FTI in physical or electronic storage will remain safeguarded to prevent unauthorized disclosures.

6) Any spoilage or any intermediate hard copy printout that may result during the processing of FTI will be given to TennCare. When this is not possible, the Contractor will be responsible for the destruction of the spoilage or any intermediate hard copy printouts and will provide TennCare with a statement containing the date of destruction, description of material destroyed, and the destruction method.

7) All computer systems receiving, processing, storing, or transmitting FTI must meet the requirements in IRS Publication 1075. To meet functional and assurance requirements, the security features of the environment must provide for the managerial, operational, and technical controls. All security features must be available and activated to protect against unauthorized use of and access to FTI.

Docusign Envelope ID: 40B7BFA4-E1BB-4360-9C9C-6FA33E97F12A

8) No work involving FTI furnished under this Contract will be subcontracted without the prior written approval of the IRS.

9) Contractor will ensure that the terms of FTI safeguards described herein are included, without modification, in any approved subcontract for work involving FTI.

10) To the extent the terms, provisions, duties, requirements, and obligations of this Contract apply to performing services with FTI, the Contractor shall assume toward any subcontractor all obligations, duties and responsibilities that TennCare under this Contract assumes toward the Contractor, and any subcontractor, shall assume toward the Contractor all the same obligations, duties and responsibilities which the Contractor assumes toward the TennCare under this Contract.

11) In addition to any subcontractor's obligations and duties under an approved subcontract, the terms and conditions of this Contract apply to all subcontractors, and all subcontractors are bound and obligated to the Contractor hereunder by the same terms and conditions by which the Contractor is bound and obligated to TennCare under this Contract.

12) For purposes of this Contract, the term "Contractor" includes any officer or employee of the Contractor with access to or who uses FTI, and the term "subcontractor" includes any officer or employee of the subcontractor with access to or who uses FTI.

13) TennCare will have the right to void the Contract if the Contractor fails to meet the terms of FTI safeguards described herein.

b. CRIMINAL/CIVIL SANCTIONS

1) Each officer or employee of the Contractor to whom FTI is or may be disclosed shall be notified in writing that FTI disclosed to such officer or employee can be used only for a purpose and to the extent authorized herein, and that further disclosure of any FTI for a purpose not authorized herein constitutes a felony punishable upon conviction by a fine of as much as five thousand dollars ($5,000) or imprisonment for as long as five (5) years, or both, together with the costs of prosecution.

2) Each officer or employee of the Contractor to whom FTI is or may be accessible shall be notified in writing that FTI accessible to such officer or employee may be accessed only for a purpose and to the extent authorized herein, and that access/inspection of FTI without an official need-to-know for a purpose not authorized herein constitutes a criminal misdemeanor punishable upon conviction by a fine of as much as one thousand dollars ($1,000) or imprisonment for as long as one (1) year, or both, together with the costs of prosecution.

3) Each officer or employee of the Contractor to whom FTI is or may be disclosed shall be notified in writing that any such unauthorized access, inspection or disclosure of FTI may also result in an award of civil damages to the IRS against the officer or employee in an amount equal to the sum of the greater of one thousand dollars ($1,000) for each unauthorized access, inspection, or disclosure, or the sum of actual damages sustained as a result of such unauthorized access, inspection, or disclosure, plus in the case of a willful unauthorized access, inspection, or disclosure or an unauthorized access/inspection or disclosure which is the result of gross negligence, punitive damages, plus the cost of the action. These penalties are prescribed by IRC sections 7213, 7213A and 7431 and set forth at 26 CFR 301.6103(n)-1. In addition to the civil damages outlined above, TennCare may pursue any potential remedy under this Contract, including but not limited to any Liquidated Damages Attachment or Exhibit, or at law or equity for Contract performance failures resulting or arising from Contractor's noncompliance with this Contract Section on IRS Safeguard of Return Information.

4) Additionally, it is incumbent upon the Contractor to inform its officers and employees of the penalties for improper disclosure imposed by the Privacy Act of 1974, 5 U.S.C. 552a.

Docusign Envelope ID: 40B7BFA4-E1BB-4360-9C9C-6FA33E97F12A

Specifically, 5 U.S.C. 552a(i)(1), which is made applicable to contractors by 5 U.S.C. 552a(m)(1), provides that any officer or employee of a contractor, who by virtue of his/her employment or official position, has possession of or access to IRS and/or TennCare records which contain individually identifiable information, the disclosure of which is prohibited by the Privacy Act or regulations established thereunder, and who knowing that disclosure of the specific material is so prohibited, willfully discloses the material in any manner to any person or agency not entitled to receive it, shall be guilty of a misdemeanor and fined not more than five thousand dollars ($5,000).

5) Granting the Contractor access to FTI must be preceded by certifying that each officer or employee understands TennCare's security policy and procedures for safeguarding FTI. The Contractor and each officer or employee must maintain their authorization to access FTI through annual recertification of their understanding of TennCare's security policy and procedures for safeguarding FTI. The initial certification and recertifications must be documented and placed in TennCare's files for review. As part of the certification and at least annually afterwards, the Contractor and each officer or employee must be advised of the provisions of IRC sections 7213, 7213A, and 7431. (See Publication 1075 Exhibit 4, Sanctions for Unauthorized Disclosure, and Exhibit 5, Civil Damages for Unauthorized Disclosure). The training on TennCare's security policy and procedures provided before the initial certification and annually thereafter must also cover the incident response policy and procedure for reporting unauthorized disclosures and data breaches. (See Publication 1075 Section 10). For the initial certification and the annual recertifications, the Contractor and each officer or employee must sign, either with ink or electronic signature, a confidentiality statement certifying their understanding of the security requirements.

c) INSPECTION

The IRS and TennCare, with 24-hour notice, shall have the right to send its inspectors into the offices and plants of the Contractor to inspect facilities and operations performing any work with FTI under this Contract for compliance with requirements defined in IRS Publication 1075. The IRS' right of inspection shall include the use of manual and/or automated scanning tools to perform compliance and vulnerability assessments of information technology ("IT") assets that access, store, process or transmit FTI. Based on the inspection, corrective actions may be required in cases where the Contractor is found to be noncompliant with FTI safeguard requirements.

E.32. Discovery and Litigation. TennCare is frequently involved in litigation as either a party or a non-party with relevant information. If any such litigation should arise, the Contractor shall cooperate fully and timely with any State attorneys or paralegals at no additional cost to the State, which shall include the following:

a. **Litigation Support**. The Contractor shall make its personnel available to testify in Tennessee, whether in person before a tribunal or by deposition. The Contractor agrees to waive any objections to any subpoena issued by a Tennessee tribunal, in any case relating to this Contract.

b. **Discovery and Litigation Hold Requirements**. The Contractor shall cooperate with all TennCare requests to aid in data and document retention and collection, as required for litigation. The Contractor shall promptly provide the State with all information within the Contractor's control if required to do so by a discovery demand or court order. The State will exert its best effort to narrow the scope of any discovery request.

The obligation to meet the requirements listed above shall survive the termination of the Contract and shall extend to any subcontractor hired by the Contractor to provide goods or perform services on its behalf as required herein.

Docusign Envelope ID: 40B7BFA4-E1BB-4360-9C9C-6FA33E97F12A

E.33. Nondiscrimination Compliance Requirements. No person on the grounds of disability, age, race, color, religion, sex, national origin, or any other classifications protected under federal or state civil rights laws shall be excluded from participation in, be denied benefits of, or be otherwise subjected to discrimination in the performance of this Contract or in the employment practices of the Contractor. The Contractor agrees to cooperate with the Division of TennCare's Office of Civil Rights ("OCRC") in carrying out its federal and state nondiscrimination compliance obligations, which include and are not limited to: the Title VI of the Civil Rights Act of 1964, Section 504 and 508 of the Rehabilitation Act of 1973, the Americans with Disabilities Act of 1990, the Age Discrimination Act of 1975, and 42 U.S.C. § 18116 (codified at 45 C.F.R. pt. 92) and Section D.9 of this Contract. The Contractor shall provide OCRC with the name and contact information for a staff member who will work with OCRC to fulfill the nondiscrimination compliance activities related to the terms of this Contract.

a. *Discrimination Complaints and Assistance.* The Contractor shall provide any discrimination complaint received relating to this Contract's services and activities within in two (2) days of receipt to OCRC at HCFA.Fairtment@tn.gov. The Contractor agrees to cooperate with OCRC and other federal and state authorities during discrimination complaint investigations and to assist individuals in obtaining information on how they can report a complaint or get assistance for a disability related need that involves TennCare's services or activities by contacting OCRC. To satisfy this obligation the Contractor may direct the individual to OCRC's webpage at: https://www.tn.gov/tenncare/members-applicants/civil-rights-compliance.html or to call TennCare Connect at 855-259-0701 if they need assistance with filing a complaint.

b. Electronic and Information Technology Accessibility Requirements. To the extent that the Contractor is using electronic and information communication technology to fulfill its obligations under this Contract, the Contractor agrees to comply with the electronic and information technology accessibility requirements under the federal civil rights laws including Section 504 and Section 508 of the Rehabilitation Act of 1973 ("Section 508"), the Americans with Disabilities Act, and 45 C.F.R. pt. 92 (or any subsequent standard adopted by an oversight administrative body, including the Federal Accessibility Board). To comply with the accessibility requirements for Web content and non-Web electronic documents and software, the Contractor shall use the most current W3C's Web Content Accessibility Guidelines ("WCAG") level AA or higher with a goal to transition to WCAG 3 level silver (For the W3C's guidelines see: https://www.w3.org/WAI/standards-guidelines/ and Section 508 standards: https://www.access-board.gov/ict/). Additionally, the Contractor agrees to comply with Title VI of the Civil Rights Act of 1964, by adding a system function that allows users to translate the content into a language other than English. This requirement may be satisfied by the provision of a link to a machine translate tool or translating the page into non-English languages as directed by TennCare.

i. The Contractor shall comply with the civil rights requirements set forth in 42 C.F.R. § 433.112 regarding the design, development, installation or enhancement of mechanized processing and information retrieval systems. In addition, the Contractor shall participate in the State's effort to comply with the nondiscrimination requirements for acquiring automatic data and processing equipment and services set forth in 45 C.F.R. § 95.633.

ii. The Contractor's accessibility responsibilities shall include ensuring optimization of the technology solution by: integrating as appropriate the concept of transversality (the ability to transition from one webpage to another webpage with the understanding for where you are navigating to), which is inherent in electronic and information technology accessibility; working with key individuals to plan accessibility at each step of the technology solution's design, development, implementation, and enhancement phases including testing and submitting evaluation reports to TennCare; appropriately allocating the accessibility project responsibilities; ensuring the accessibility technical and functional criteria are met at every milestone that contains an accessibility component for the technology solution; understanding the difference between accessible content and conforming content; being aware of the technology solution's testing tools and any limitations the tools have for testing accessibility

Docusign Envelope ID: 40B7BFA4-E1BB-4360-9C9C-6FA33E97F12A

and providing workarounds; and assessing the impact of technology platforms on the technology solution (i.e., applications, portals, and tools should work and be accessible across different platforms).

iii. Contractor agrees to perform regularly scheduled (i.e., automatic) scans that will occur at a minimum on a monthly basis and manual testing for the most current WCAG level AA or higher accessibility guidelines (WCAG 3.0 Silver) for all user content and applications in order to meet the standards for compliance. The Contractor must ensure that any system additions, updates, changes or modifications comply with the most current WCAG level AA or higher accessibility guidelines (WCAG 3.0 Silver). Commercial Off-the-shelf ("COTS") products may be used to verify the technology solution's compliance with the most current WCAG level AA or higher accessibility guidelines (WCAG 3.0 Silver). The reports shall be provided to TennCare's Office of Civil Rights Compliance ("OCRC") for review and approval.

iv. Should the system or a component of the system fail to comply with the accessibility standards, the Contractor shall develop and submit to OCRC for approval a noncompliance report that identifies the areas of noncompliance, a plan to bring the system or component into compliance, an alternative/work around that provides users with the equivalent access to the content, and a timeframe for achieving that compliance. OCRC shall review the noncompliance report to determine whether or not it is acceptable and should be implemented. Once the noncompliance report is approved by OCRC the Contractor may implement the compliance plan. OCRC, in its sole discretion, shall determine when a satisfactory compliance plan resolution has been reached and shall notify the Contractor of the approved resolution. If Contractor is unable to obtain content that conforms to the most current WCAG level AA or higher accessibility guidelines (WCAG 3.0 Silver), it shall demonstrate through its reporting to OCRC that obtaining or providing accessible content would fundamentally alter the nature of its goods and services or would result in an undue burden.

v. The Contractor shall have a designated staff member responsible for Contractor's electronic and information technology accessibility compliance. The name and contact information for this individual shall be provided to OCRC within ten (10) days of the implementation phase of this Contract and within ten (10) days of this position being reassigned to another staff member.

vi. Prior to the start of this Contract and on an annual basis thereafter, the Contractor's staff that is designated to work on TennCare's electronic and information technology projects shall receive training on electronic and information technology accessibility requirements. The Contractor shall be able to show documented proof that this training was provided. In addition, Contractor shall provide a copy of its electronic and information technology accessibility training to OCRC upon request.

IN WITNESS WHEREOF,

INSPIRA ENTERPRISE, INC.:

Signed by:
Amit Gandre
5100B80A4ECA44E...

3/7/2025

CONTRACTOR SIGNATURE **DATE**

Docusign Envelope ID: 40B7BFA4-E1BB-4360-9C9C-6FA33E97F12A

Amit Gandre CEO, Americas

PRINTED NAME AND TITLE OF CONTRACTOR SIGNATORY (above)

STATE OF TENNESSEE
DEPARTMENT OF FINANCE AND ADMINISTRATION
DIVISION OF TENNCARE:

Jim Bryson / JB 3/25/2025

JIM BRYSON, COMMISSIONER **DATE**

Docusign Envelope ID: 40B7BFA4-E1BB-4360-9C9C-6FA33E97F12A

DEFINITIONS AND ABBREVIATIONS

Docusign Envelope ID: 40B7BFA4-E1BB-4360-9C9C-6FA33E97F12A

1.0 DEFINITIONS AND ABBREVIATIONS

For the purposes of the Managed Security Operations Center (SOC) Services Request for Proposal (RFP) and resulting Contract, the following definitions of terms shall apply, unless otherwise indicated. All Deliverables not defined here shall be as defined in the MSS TennCare Solution Implementation Lifecycle RACI and Deliverables document included in Attachment C: Procurement Library and Table 3: Table of Deliverables in the Contract.

Definitions

Term	Definition
Acceptance	A notice from TennCare to the Contractor that a Deliverable or Service has conformed to its applicable Acceptance criteria in accordance with the process described in the TennCare Solution Implementation Lifecycle (SILC) RACI and Deliverables.
Artifacts	Documents created by the project to describe the Solution or service being implemented and the processes used to define, implement, and manage the Solution.
Authorized User	A person or role that has specified access rights to a given area, system, or sub-system.
Benefits	The advantage gained from having used the Solution, to be confirmed post-implementation.
Breach	The loss of control, compromise, unauthorized disclosure, unauthorized acquisition, or any similar occurrence where a person other than the authorized user accesses or potentially accesses personally identifiable information, protected health information or Federal tax information.
Business Days	Monday through Friday from 8:00 AM – 5:00 PM Central Time; TennCare holidays are excluded. A list of TennCare Holidays can be located at https://www.tn.gov/about-tn/state-holidays.html#:~:text=Tennessee%20State%20Government%20Holiday%20Office%20Closures.%201%20Friday%2C,and%20Friday%2C%20December%2024%20%E2%80%93%20Christmas%20%2A%2A.%20
Business Processes	Structured set of activities designed to accomplish a specific objective, turning inputs into defined outputs. It may include roles, responsibilities, tools, and management controls required to deliver outputs.
Business Report	Organized, written statement of facts related to a business matter.
Centers for Medicare and Medicaid Services (CMS)	The organizational unit of the U.S. Department of Health and Human Services responsible for administration of the Title XIX and Title XXI Programs under the Social Security Act.
Change Order	A written form, in response to a Change Request that is mutually agreed to by TennCare and the Contractor, which modifies, deletes, or adds to the deliverables or services, in whole or in part, and that is made in accordance with the Change Order terms as defined by TennCare.
Change Request	A written form used to propose that the Deliverables or Services be modified, deleted, or added to, in whole or in part, made in accordance with the Change Request terms as defined by TennCare.
Children's Health Insurance Program (CHIP)	Children's Health Insurance Program (CHIP) authorized under Title XXI of the Social Security Act. CHIP provides low-cost health coverage to children in families whose incomes exceed the standard limits to qualify for Medicaid. Tennessee's CHIP is referred to as CoverKids.

Docusign Envelope ID: 40B7BFA4-E1BB-4360-9C9C-6FA33E97F12A

Claim	A record of performed services and payment requested from a provider for health care services provided to a TennCare Member.
CMS Certification	The CMS-written acknowledgement that the MMIS Core Modular Solution meets all legal and operational requirements necessary for Enhanced Federal Financial Participation (EFFP).
Commercial Off-the-Shelf (COTS)	A software that already exists and is available from commercial sources. It is also referred to as off-the-shelf and is ready to use without any modification by the user. Examples of COTS software include, but are not limited to, SaaS, and commercially available cloud-native services and solutions, such as Amazon Web Services (AWS).
Confidential Information	Any non-public, confidential, or proprietary information, whether written, graphic, oral, electronic, visual, or fixed in any tangible medium or expression, supplied by TennCare. This includes individuals enrolled in any TennCare program or relating to individuals who may be potentially enrolled in a TennCare program, to the extent that confidential status is afforded such information under State and/or Federal laws or regulations. All confidential information shall not be subject to disclosure under the Tennessee Public Records Act.
Confidentiality	Preserving authorized restrictions on information access and disclosure, including means for protection personal privacy and proprietary information.
Configuration Item (CI)	Any component that needs to be managed in order to deliver an IT service.
Configuration Management	The process of documenting formal procedures to apply technical and administrative direction and surveillance to: identify and document the functional and physical characteristics of a product, result, service, or component; control any changes to such characteristics; record and report each change and its implementation status; and support the audit of the products, results, or components to verify conformance to requirements. It includes the documentation, tracking systems, and defined approvals necessary for authorizing and controlling changes. Configuration Management Controls include but are not limited to: — **CM-2**: Detailed configuration settings consistent with CM-2 (Configuration Management as per NIST 800-53) that satisfy the required CMS baseline configurations. — **CM-6**: Detailed configuration settings consistent with CM-6 (Configuration Management as per NIST 800-53) that satisfy the required CMS baseline configurations. — **CM-8**: Equipment listing consistent with CM-8 (Configuration Management as per NIST 800-53) that supports the system/application.
Continental United States	Terms used to describe 48 states and District of Columbia in the United States, excluding Hawaii and Alaska.
Continuous Improvement Process (CIP)	An ongoing effort to make incremental improvements to products, Services, or processes over time. Continuous Improvement is done by assessing processes and practices for efficiency, accuracy, and effectiveness.

Docusign Envelope ID: 40B7BFA4-E1BB-4360-9C9C-6FA33E97F12A

Contractor	The entity performing Services pursuant to this Contract, including any officer, owner, Member, director, employee, volunteer, agent, subcontractor, representative, or assignee of the Contractor, and any other person, partnership, corporation, or other legal entity performing work or Services, or providing materials, under this Contract for or on behalf of the Contractor. For purposes of any permitted subcontract, "Contractor" includes any subcontractor(s), owners, Members, officers, directors, partners, employees, and/or agents.
Dark Web	The part of the internet that isn't visible to search engines and requires the use of an anonymizing browser called Tor to be accessed
Dashboard	A visual representation of the results of a query run on data. A Dashboard brings together useful information on a series of screens and/or web pages. Information contained in a dashboard includes, but is not limited to, reports, web links, calendar, news, tasks, e-mail, etc.
Data Governance	Aligns the organization with the business strategy and enables prioritization and approval of initiatives and a plan for the introduction of processes which will continuously monitor and improve Data Quality.
Data Loss Prevention	Data Loss Prevention is the implementation of security controls and policies, such as regulatory compliance, intellectual property protection, and consistent reporting and monitoring practices, to protect from the leakage, disappearance, or damage of data that an organization holds, with an emphasis on protection against high profile data leakage of sensitive data such as PII or PHI.
Data Mining	The process of examining large data stores to identify patterns or extract usable data.
Data Model	A Data Model represents types of data and their organization in response to data requirements. Data Models may be implemented in Databases or may just be used for communicating data requirements independent of how those requirements will be physically implemented. Data Modelling is also a design activity that through best practices, reference models, experience, and design choices, results in the best organization of data requirements.
Database	A collection of information stored in an organized, structured manner for fast and convenient search and retrieval by business applications and Business Intelligence software.
Defect	Any nonconformance of the goods or services to the terms and conditions of the Contract. A Defect may include issues that occur with the solution at the Component or sub-system level and may lead to a failure (deeming the solution "Defective"). A Defect can exist within testing and production environments, resulting in non-conformance of the design and/or requirements associated with the solution.
Deliverables	All Services, tangible, and intangible products TennCare intends the Contractor to produce, prepare, and deliver during the course of the Contractor's performance under this Contract, including those described in the RFP and the TennCare Solution Implementation Lifecycle (SILC) RACI and Deliverables.
Implementation	The phase encompassing the MSS-implementation of required business and technical functionality.

Docusign Envelope ID: 40B7BFA4-E1BB-4360-9C9C-6FA33E97F12A

Disaster	An unplanned interruption of the IT infrastructure Components used to support Business Processes. Disasters include, but are not limited to the following: bomb threat, civil disturbance, cyber incident, earthquake, internal fire, external fire, internal flood, external flood, generator failure, hazmat exposure, ice event, pandemic, power outage, prolonged IT outage, severe thunderstorm, temperature extremes, tornado, workplace violence, and utility failure (e.g. HVAC, water, gas, etc.).
Electronic and Information Technology	Also referred to as Information and Communication Technology (ICT), Electronic and Information Technology refers to information technology and other equipment, systems, technologies, or processes, for which the principal function is the creation, manipulation, storage, display, receipt, or transmission of electronic data and information, as well as any associated content. Examples of ICT include, but are not limited to: computers and peripheral equipment; information kiosks and transaction machines; telecommunications equipment; customer premises equipment; multifunction office machines; software; applications; Web sites; videos; and, electronic documents. See 36 C.F.R. Pt. 1194, App. A.
Eligibility	A series of requirements and related Business Processes that determine whether an individual is eligible for Medicaid Benefits.
Enterprise-Wide	Encompassing the entire TennCare organization that is inclusive of all programs and Services under the scope of this RFP and subsequent Contract, rather than a single business department or function.
Enterprise-Wide	Throughout the entire business.
Event	An Event is defined as any Incident that has significance for the management of an IT service or other Configuration Item.
Event Management	The process that monitors all Events that occur through the IT infrastructure, thereby allowing for normal operation and also detecting and escalating exception conditions.
False Positive Ticket Reports	Reports identifying instances where a threat or breach was detected and identified as malicious even though it isn't a threat.
Federal Tax Information (FTI)	Any information derived from federal or state tax returns protected under confidentiality provisions of Internal Revenue Code section 6103.
Functional Requirement	A requirement that defines specific behaviors or functions the contracted MSS must perform as part of the Contract.
Gate Review	A phase-driven go/no-go decision point where project activities are reviewed to assure that appropriate requirements are observed. A project cannot proceed without a "Go" decision by the appropriate TennCare management for a specific stage gate. Gate Reviews will be conducted in accordance with the processes described in the TennCare Solution Implementation Lifecycle (SILC).
Go-Live	An Event when a Solution functionality is deployed and made available in a production environment for operational usage.
Graphical User Interface (GUI)	The screen that enables users to interact with a system through graphical icons and audio indicators, such as text or buttons.
Health Information Technology for Economic and Clinical Health (HITECH)	The federal law enacted as part of the American Recovery and Reinvestment Act (ARRA) of 2009 to promote the adoption and meaningful use of health information technology.
Health Insurance Portability and Accountability Act (HIPAA)	The federal law enacted in 1996 which includes requirements to protect patient privacy, security of electronic medical records, and to prescribe methods and formats for exchange of electronic medical information.
Incident	An occurrence that actually or potentially jeopardizes the confidentiality,

Docusign Envelope ID: 40B7BFA4-E1BB-4360-9C9C-6FA33E97F12A

	integrity or availability of an information system or the information system processes, stores, or transmits or that constitutes a violation or imminent threat of violation of security policies, security procedures or acceptable use policies.
Incident Management	The process responsible for managing the lifecycle of all Incidents. The purpose of Incident Management is to restore normal service operations as quickly as possible and minimize the adverse impact on business operations, thus ensuring that agreed levels of service quality are maintained.
Incident Response	The process of detecting, managing, and recovering from cyberattacks and security breaches.
Indicators of Compromise (IOCs)	Indicator of compromise (IOC) is information indicating that an incident may have occurred or may be in progress
Industry Standards and Policies	A set of criteria within an industry relating to the standard functioning and carrying out of operations in their respective fields of production. It is the generally accepted requirements followed by the members of an industry.
Information Technology Infrastructure Library (ITIL)	ITIL is an acronym for the Information Technology Infrastructure Library (ITIL), a globally recognized collection of best practices for IT Service management that focuses on aligning IT Services with the needs of business.
Information Technology Service Management (ITSM)	A strategic approach for designing, delivering, managing, and improving the way information technology (IT) is used within an organization. The goal of IT Service Management (ITSM) is to ensure that the right processes, people, and technology are in place so that the organization can maximize business value from the use of information technology.
Information Technology Service Management (ITSM)	Activities performed by an organization to design, develop, and operate IT services.
Interface	A bi-directional integration between TennCare ticketing system and MSS ITSM to achieve below tasks: All alerts that triggered in Splunk must create a ticket in TennCare ticketing system and MSS ITSM All comments added to either of ticketing system must be reflected in the other
Integration Services (IS)	Services focused on establishing and maintaining interoperability through the use of the integration platform, which enables secure real-time, or close to real-time, data exchange and integration of data and Services across system boundaries.
Integrity	Guarding against improper information modification or destruction, including ensuring non-repudiation and authenticity.
IRS Pub 1075	IRS Pub 1075 provides guidance to ensure the policies, practices, controls, and safeguards employed by recipient agencies, agents, or contractors adequately protect the confidentiality of FTI
Key Personnel	The Contractor personnel deemed by TennCare to be essential throughout the contract lifecycle to satisfactory adhere to demonstratable performance of the requirements contained within the Contract as described in the Key Personnel Table in A.12.2.5.
Least privileged principal	Least privileged principal is an information security concept which maintains that a user or entity should only have access to the specific data, resources and applications needed to complete a required task.
Limited English Proficient (LEP)	Individuals who do not speak English as their primary language and who have a limited ability to read, write, speak, or understand English and may be eligible to receive language assistance with respect to a particular type of service, benefit, or encounter.

Docusign Envelope ID: 40B7BFA4-E1BB-4360-9C9C-6FA33E97F12A

Liquidated Damages	A clause that specifies a predetermined amount of money that must be paid as damages for failure to perform under a contract.
Log source	A data source that creates an event log
Major Incidents	A highest-impact, highest-urgency incident that affects a large number of users, depriving the business of one or more crucial services
Managed Security Services (MSS)	Oversight and administration of an Enterprise's security processes.
Medicaid	The Federal medical assistance program authorized in Title XIX of the Social Security Act, administered by states and U.S. Territories.
Medicaid Modernization Program (MMP)	MMP is an all-encompassing term used to describe TennCare's various initiatives and projects aimed at streamlining its Medicaid program to improve operational efficiencies and service delivery through industry-leading enabling technologies.
Member	A person who has been deemed eligible to receive health coverage Benefits under the TennCare Medicaid-program.
Minimum Acceptable Risk Standards for Exchanges (MARS-E)	A document suite of guidance, requirements, and templates assembled by CMS. The document suite contains implementation standards for key security requirements contained in Department of Health and Human Services (HHS) Affordable Care Act (ACA) Regulations (45 CFR §§155.260 and 155.280) and other State and Federal regulations and policies. This is a harmonized set of guidelines inclusive of CMS and IRS requirements. Any reference to this package, even under CMS context references, should also infer compliance with current IRS Safeguards Program and IRS Pub 1075, where applicable by usage of data type and/or classification.
Non-Functional Requirement	A requirement that specifies criteria that can be used to validate the operation of a Solution, rather than specific Solution behaviors. Non-Functional requirements evaluate if the Solution is "fit for use."
Open-Source	Software where the original source code is made freely available and can be redistributed or modified.
Operational Readiness Review (ORR)	A review to ensure that the system is being implemented into production and is ready for Go-Live. System readiness, organizational change management, and outreach activities are also verified.
Operational Readiness Testing (ORT)	A technical testing activity to ensure that a MMIS Module, integrated with other MMIS Modules or Solutions, complies with Non-Functional Requirements.
Operations & Maintenance (O&M) Phase	Maintenance and support Services that will be performed by a Contractor to improve performance or other attributes associated with the Contractor's MMIS Module.
Payment	The amount(s) to be paid for deliverables and Services provided under this Contract, in whole or in part, as described in the Cost Proposal and Section C of the *Pro Forma* Contract, and any subsequent written amendments or Change Orders.
Personally Identifiable Information (PII)	Information that can be used to identify a specific individual, either alone or when combined with other information, such as birth dates, biometric records, or social security numbers.
Plan of Action and Milestones (POA&M) Report	Document that identifies tasks that need to be accomplished. It details resources required to accomplish the plan, milestones for meeting tasks, and the scheduled completion dates for each milestone.
Playbook	A Playbook is a set of processes that defines how to respond to a certain type of security incident.
Privacy	The assurance that the confidentiality of, and access to, certain information about an entity is protected

Docusign Envelope ID: 40B7BFA4-E1BB-4360-9C9C-6FA33E97F12A

Problem	A cause, or potential cause, of one or more Incident(s) and associated Defect(s) classification(s). Problem(s) can be raised in response to a single significant Incident and assigned Defect classification (Critical, High, Medium or Low) or multiple similar Incidents and assigned Defects (regardless of classification level). Problem(s) can also be raised without the existence of a corresponding Incident, where a Defect categorization has solely been assigned (e.g. bug-fixing).
Protected Health Information (PHI)	Individually identifiable health information that is transmitted by electronic media, maintained in electronic media, or transmitted or maintained in any other form.
Provider	An institution, facility, agency, person, corporation, partnership, or association which is enrolled with the TennCare Program to accept and provide covered Services to eligible TennCare Members.
Quality Assurance Testing	The process of ensuring the software or service meets quality standards to deliver consistent and efficient results.
Quarter	3-month period beginning from the effective date
Quarterly Payment	The point-in-time in which TennCare will pay the agreed upon cost for Services.
Regression Testing	A form of software testing used to confirm or deny that previously tested software functionality continues to meet acceptance criteria after the software undergoes changes. TennCare requires that software be regression tested to confirm that the quality of the system has not regressed. Regression testing is performed prior to each subsequent release into a Production environment. Each vendor is required to establish a regression test-suite in collaboration with TennCare IS and appropriate business representation, to perform regression-execution for each subsequent release, and to provide regression results for review supporting a Release Readiness “Go/No-Go” stakeholder decision allowing deployment into Production.
Security Information Event Management (SIEM)	The process of identifying, monitoring, recording, and analyzing security events or incidents within a real-time IT environment. A SIEM provides a comprehensive and centralized view of the security scenario of an IT infrastructure.
Security Operations Center (SOC)	A command center facility for a team of IT professionals with expertise in information security who monitors, analyzes, and protects an organization from cyber-attacks. Also called Managed Security Operations Center (MSOC).
Security Orchestration, Automation, and Response (SOAR)	SOAR platforms helps organizations to coordinate, execute and automate tasks between various people and tools all within a single platform
Security policy	A rule or set of rules that govern the acceptable use of an organization's information and services to a level of acceptable risk and the means for protecting the organization's information assets.
Sensitive Data	Any data or record that identifies a person, including health information or financial information, and any data or record designated as sensitive, proprietary, or confidential by TennCare, State, or Federal law or regulation. Examples of sensitive data includes, but is not limited to, PII (Personally Identifiable Information), SPII (Sensitive Personally Identifiable Information), PHI (Protected Health Information), SSA (Social Security Administration), CJIS (Criminal Justice Information Services), TBI (Tennessee Bureau of Investigation), and FTI (Federal Tax Information).

Docusign Envelope ID: 40B7BFA4-E1BB-4360-9C9C-6FA33E97F12A

Service Design	An ITIL service lifecycle stage encompassing the design of new services, as well as changes and improvements to existing services, that are fit for purpose, fit for use, and that can be delivered by the organization and its ecosystem.
Service Desk	The single point of contact between the service Provider and the users. A typical Service Desk manages Incidents and service requests, and also handles communication with the users.
Service Level Agreement (SLA)	An instrument to measure performance expectations between TennCare and the Contractor that detail the characteristics, quality, delivery standards, timeframe, and/or scope of services to be provided.
Service Lifecycle	An approach to IT Service Management (ITSM) that emphasizes the importance of coordination and control across the various functions, processes, and systems necessary to manage the full lifecycle of IT services.
Services	Any and all Services, Deliverables, materials, Special Project Change Orders, Enhancement Change Orders, and any other work requirement to be performed by the Contractor pursuant to the Contract.
SIEM Engineering Team	Team responsible for providing technical support and engineering for network/cloud firewalls, network/cloud intrusion detection/prevention system, virtual private networks, and web security gateways.
Social Security Administration (SSA)	Government agency that administers social programs, covering disability, retirement, and survivor's benefits.
Software as a Service (SaaS)	Software as a Service (SaaS) is a software licensing and delivery model in which software is licensed for use, on a subscription basis and is cloud hosted. Instead of installing and maintaining software, TennCare will simply access it via the Internet, freeing itself from software and hardware management.
Solution	The entirety of the system elements or components, including the code, configuration, software, data, and applications that are connected as a whole, and are necessary to provide autonomous operation of all required functions.
Solution Vendor	A TennCare contractor, including its subcontractors, that provide a complete system (containing a combination of hardware, software, and services) as a result of a TennCare competitive IT procurement. TennCare Solution Vendor systems include but are not limited to: Current TennCare Solutions • Systems Integration Services Support for Eligibility Modernization Project; • Integration Services; • Cloud-Based Decision Support System for the Data Ecosystem Solution; • Cloud-Based Data Ecosystem Enterprise Data Warehouse; • Cloud Based Master Data Management Data Ecosystem; • Cloud-Based Data Ecosystem Data Quality/Extract-Transform-Load Pipeline; • Closed Loop Referral System; • Medicaid Management Information System Core Modular Solution (all module contracts); • Technical Advisory Services for Medicaid Modernization Program; • Information Technology Audit Management; • MMIS – Program Integrity; • Pharmacy Benefits Management (PBM) Services;

Docusign Envelope ID: 40B7BFA4-E1BB-4360-9C9C-6FA33E97F12A

	• Maintenance and Operation of HCFA Provider Registration Portal; • Medicaid Management Information Systems (MMIS); and • TennCare Dental Benefit Management (DBM) Programs Upcoming TennCare Solutions • Workforce Registry RFP #31865-00658; • Provider Solution Services RFP #31865-00652; • Tennessee Eligibility Determination System RFP #31865-00648; • Value Based Payment (VBP) Program Consulting Services RFP #31865-00647; • Pharmacy Benefits Administration (PBA) RFP #31865-00654; and • Care Coordination Tool (CCT) RFP #31865-00653 In the event TennCare creates a new Solution Vendor system or re-procures an existing Solution Vendor system after the Contract Effective Date, the SOC Contractor and its subcontractors will be notified of its prohibition from bidding on or serving as a subcontractor on such Solution Vendor contract.
Solution Implementation Lifecycle (SILC)	Defines the phased approach to solution implementation projects. The TennCare SILC details the Gate Review process, outlines the entry and exit criteria of requirements, defines Contractor activities and coordination responsibilities, and aligns associated Deliverables for each Gate in the lifecycle.
Splunk User Interface	Default window that interacts with the user.
Strategic Technology Solutions (STS)	A division within the State of Tennessee, Department of Finance & Administration (F&A), that provides planning, resources, execution, and coordination in managing the information systems needs of TennCare.
Tabletop exercise	A discussion-based exercise where personnel meet in a classroom setting or breakout groups and are presented with a scenario to validate the content of plans, procedures, policies, cooperative agreements or other information for managing an incident.
Takeover	The continuation of a Solution and/or Services from an incumbent contract/Contractor.
TennCare	TennCare is the State of Tennessee agency responsible for the administration of the Medicaid and Children's Health Insurance Programs. A list of TennCare programs is located at: https://www.tn.gov/tenncare/members-applicants/eligibility/categories.html.
TennCare Enterprise Knowledge Management Strategy	As a component of TennCare continuous improvement practices, TennCare has instituted processes that require vendor partners to document project Artifacts and best practices. TennCare has established processes for both TennCare and vendor partner's engagement to provide knowledge sharing associated with TennCare-designated project engagement activities.
TennCare Governance Standards	TennCare Governance Standards provide guidance, and the framework for a Solution's conformance to State policies, expectations and intentions related to Solution Implementation Lifecycle (SILC) activities and requirements. Additional policy and procurement documentation may be incorporated by TennCare, in accordance with the Contract, at any point in the Contract Term to align with enterprise governance requirements, specifications, or policies as dictated by TennCare or

Docusign Envelope ID: 40B7BFA4-E1BB-4360-9C9C-6FA33E97F12A

	other State or Federal entities. Current TennCare Governance Standards are included in Attachment C, Procurement Library.
TennCare Security and Privacy Offices	The areas of TennCare responsible for oversight of all enterprise solution security and privacy standards.
TennCare Security, Orchestration, Automation, and Response (SOAR) Platform	A collection of security software solutions and tools for browsing and collecting data from a variety of sources.
TennCare's Office of Civil Rights Compliance	Office primarily concerned with enforcing civil rights laws, policies, and procedures and ensuring fairness under the TennCare program.
Tennessee Department of Finance and Administration (F&A)	The State agency that oversees all State spending and acts as the chief corporate office of the State.
Threat Hunting	Threat hunting is the practice of proactively searching for cyber threats that are lurking undetected in a network.
Threat Intelligence	The collecting, processing, organizing, and analyzing data into actionable information that relates to capabilities, opportunities, actions, and intent of adversaries in the cyber domain to meet a specific requirement determined by and informing decision-makers.
Ticket Enrichment	Enhancing alerts by adding more intel for IOCs (virus total, Threatconnect), ticket correlation and adding a link to the corresponding playbook for the alert that is triggered Ticket correlation - alerts with similar user names, IPs, host names etc are linked to the latest alert that is triggered
Ticketing System	Software application that manages and tracks customer support requests and issues.
Tier I – Service Desk	The Tier I – Service Desk is managed by the IS Contractor and supports general issues, such as receiving initial calls, password reset requests, and identifying incidents. If the request or Incident cannot be addressed at the Tier I – Service Desk level, the Tier I – Service Desk is responsible for the routing of higher complexity issues requiring Tier II – Level Support to the appropriate IS Component and/or MMIS Module Support Team. Additionally, the Tier I – Service Desk is responsible for tracking, recording, and closing every Incident.
Tier II – Level Support	Tier II – Level Support is provided by the Contractor's technicians who have the technical-, application-, or component-specific knowledge and troubleshooting capabilities beyond Tier I – Service Desk general support. If there is an existing issue, Tier II – Level Support identifies a Solution or a workaround and is responsible for reporting the resolution to the Tier I – Service Desk. If there is no solution or workaround, the Tier II – Level Support shall add an entry into the ITSM tool. The IS Contractor is responsible for resolving Incidents at the ISL application level, such as, but not limited to, inter-module issues related to application connection. If the origin of the incident is ISL-related and cannot be resolved at the Tier II – Level Support, the Incident will be routed to Tier III – Level Support for ISL technical expertise. If the origin of the Incident is MMIS Module-related, the Incident will be escalated to the appropriate MMIS Module Support Team.
Tier III – Level Support	Tier III – Level Support requires resources with technical expertise and specialized skills above Tier II – Level Support and is usually provided by specialists with deep product knowledge to address Incidents such as critical workflow malfunctions or inability to complete a transaction. Once an Incident or Problem has been resolved, or a workaround has been identified, the Tier III – Level Support will report resolution results to the

Docusign Envelope ID: 40B7BFA4-E1BB-4360-9C9C-6FA33E97F12A

	Tier I – Service Desk level.
Turnover	Describes all activities involved in transitioning the MSS and responsibilities to TennCare, a designated Contractor, and/or successor Contractor at the end of the Contract term.
Turnover Plan	Documentation that describes how the MSS solution is transitioned to another vendor or to TennCare for continued operation.
Unit Testing	A testing activity where the Contractor performs technical testing internal to their Solution.
Use Case	A use case can be technical rules or conditions applied on logs that are ingested into the SIEM to detect threats
User Acceptance Testing (UAT)	A testing activity carried out by end-users to ensure that the Solution meets business needs from end-to-end.
User Interface (UI)	The User Interface is the point of human-computer interaction and communication on a device, webpage or application
Virtual Private Network (VPN)	A data network that enables two or more parties to communicate securely across a public network by creating a private connection, or "tunnel," between them.
Warranty Defect	Any nonconformance of the goods or Services to the terms and conditions of the Contract within the Warranty Period. A Warranty Defect is classified as Critical, High, Medium, and Low and must be resolved in the given timeframe listed in Contract Attachment B, Service Level Agreements and Liquidated Damages.
Workflow	The processes involved in completing an assignment or functional job, including activities such as the organization of resources or personnel; the design and association of tasks; the development of procedures (and their implementation); execution, followed by feedback, oversight, and quality improvement.

Abbreviations

Abbreviation	Definition
24x7x365	Available twenty-four (24) hours per day, seven (7) days per week, and three hundred sixty-five (365) days per year
276	276 Encounter Status Inquiry
277CA	277CA Claim Acknowledgment Transaction
3NF	Third Normal Form
AC	Access Controls
ACA	Affordable Care Act
ACH	Automated Clearing House
ADA	Americans with Disabilities Act
ASCII	American Standard Code for Information Interchange
AUP	TennCare's Acceptable Use Policy
API	Application Programing Interface

Docusign Envelope ID: 40B7BFA4-E1BB-4360-9C9C-6FA33E97F12A

APT	Advanced Persistent Threat
ARRA	American Recovery and Reinvestment Act of 2009
ASC X12 820	820 HIPAA Transaction Set
BC/DR	Business Continuity/Disaster Recovery
BPM	Business Processes Management
BRE	Business Rules Engine
BRM	Business Rules Management
CAP	Corrective Action Plan
CAQH	Council for Affordable Quality Healthcare
CAQH-CORE	Council for Affordable Quality Healthcare - Committee on Operating Rules for Information Exchange
CASB	Cloud Access Security Broker
CBT	Computer Based Training
CD	Control Directive
CFR	Code of Federal Regulations
CHIP	Children's Health Insurance Program
CI	Configuration Item
CIP	Continuous Improvement Process
CISM	Certified Information Security Manager
CISO	Chief Information Security Officer
CISSP	Certified Information Systems Security Professional
CM	Control Memorandum
CMPPA	Computer Matching and Privacy Protection Act of 1988
CMS	Centers for Medicare and Medicaid Services
CORE	Committee on Operating Rules for Information Exchange
CONUS	Continental United States
COTS	Commercial Off-the-Shelf
CPO	Central Procurement Office
CPU	Central Processing Unit
CSF	Common Security Framework
CSV	Comma-Separated Values
DB	Database
DDI	Design, Development, and Implementation
DDoS	Distributed Denial of Service
DE	Data Ecosystem
DED	Deliverable Expectation Document
DNS	Domain Name System
DUNS	Data Universal Numbering System
EAI	Enterprise Application Integration
ECM	Enterprise Content Management
EDI	Electronic Data Interchange Gateway
EDR	Endpoint Detection and Response
EFFP	Enhanced Federal Financial Participation
EFT	Electronic Funds Transfer
EP	Encounter Processing
ETL	Extract-Transform-Load
eTMO	Enterprise Test Management Office

Docusign Envelope ID: 40B7BFA4-E1BB-4360-9C9C-6FA33E97F12A

ESB	Enterprise Service Bus
ESP	TennCare Enterprise Security Policy
FFATA	Federal Funding Accountability and Transparency Act
FHIR	Fast Healthcare Interoperability Resources
FIPS	Federal Information Processing Standard
FM	Financial Management
FIM	File Integrity Management
FMAP	Federal Medical Assistance Percentage
FMDS	Financial Module Data Store
FTI	Federal Tax Information
FTP	File Transfer Protocol
FTPS	File Transfer Protocol with support for Transport Layer Security
US GAAP	United States Generally Accepted Accounting Principles
GAAP	Generally Accepted Accounting Principles
GIAC	Global Information Assurance Certification
GLBA	Graham-Leach-Bliley Act of 1999
G0-DBE	Governor's Office of Diversity Business Enterprise
GUI	Graphical User Interface
GRC	Governance Risk and Compliance
HHS	U.S. Department of Health and Human Services
HDH	Head of Household
HEDIS	Healthcare Effectiveness Data and Information Set
HL7	Health Level Seven
HIPAA	Health Insurance Portability and Accountability Act of 1996
HITECH	Health Information Technology for Economic and Clinical Health Act
HITRUST	Health Information Trust Alliance
HTML	Hypertext Markup Language
IAM	Identity and Access Management
ICN	Internal Control Number
IEA	Information Exchange Agreement
IDPS	Intrusion Detection and Prevention System
IMB	Intelligent Mail Barcode
IOCs	Indicators of Compromise
IRC	Internal Revenue Code
IRP	Contractor's Incident Response Plan
IRS	Internal Revenue Service
IS	Integration Services
ISL	Integration Services Layer
ISPP	TennCare Information Security Program Plan
IT	Information Technology
ITIL	Information Technology Infrastructure Library
ITSM	Information Technology Service Management
JSON	JavaScript Object Notation
KPI	Key Performance Indicator

Docusign Envelope ID: 40B7BFA4-E1BB-4360-9C9C-6FA33E97F12A

LD	Liquidated Damage
MARS-E	Minimum Acceptable Risk Standards for Exchanges
MCC	Managed Care Contractor
MCO	Managed Care Organization
MDM	Master Data Management
ME	Member Enrollment
MFA	Multi-Factor Authentication
MFT	Managed File Transfer
NGFW	Next Generation Firewall
MIC	Medicaid Integrity Contractors
MITA	Medicaid Information Technology Architecture
MMIS	Medicaid Management Information System
MMP	Medicaid Modernization Program
MMPVP	Medicaid Modernization Program Vendors and Partners
MS-ISAC	Multi State Information Sharing and Analysis Center
NACHA	National Automated Clearinghouse Association
NCCI	National Correct Coding Initiative
NCPD	Notice of Calculation of Potential Damages
NCPDP	National Council for Prescription Drug Programs
NIAD	Notice of Intent to Assess Damages
NIEM	National Information Exchange Model
NIST	National Institute of Standards and Technology
NPD	Notice of Potential Damages
NOC	Network Operations Center
O&M	Operations and Maintenance
OCRC	TennCare's Office of Civil Rights Compliance
ODBC	Open Database Connectivity
OIG	Office of Inspector General
OWASP	Open Web Application Security Project
PC	Personal Computer
P-Card	State Purchasing Card
PDF	Portable Document Format
PERM	Payment Error Rate Measurement
PHI	Protected Health Information
PII	Personally Identifiable Information
PMP	Project Management Plan
PMPM	Per Member Per Month
POA&M	Plan of Actions and Milestones
PPACA	Patient Protection and Affordable Care Act
RACI	Responsible, Accountable, Consulted, and Informed
RDA	Records Disposition Authorization
RFP	Request for Proposals
RFQ	Request for Qualifications
RPA	Robotic Process Automation
RPP	Rapid Payment Processing
RTM	Requirements Traceability Matrix
SFTP	Secure (Shell) File Transfer Protocol
SIEM	Security Incident Event Management
SILC	Solution Implementation Lifecycle
SIT	System Integration Testing
SLA	Service Level Agreement
SME	Subject Matter Expert

Docusign Envelope ID: 40B7BFA4-E1BB-4360-9C9C-6FA33E97F12A

SOA	Service Oriented Architecture
SAP	CMS Security and Privacy Assessment Plan
SOP	Standard Operating Procedure
SPMO	Strategic Program Management Office
SPSS	Statistical Package for the Social Sciences
SQL	Structured Query Language
SSA	United States Social Security Administration
SSO	Single Sign-On
SSP	System Security Plan
STS	Strategic Technology Solutions
TARB	TennCare Architecture Review Board
TCA	Tennessee Code Annotated
TCS	Transactions and Code Sets
TCRS	Tennessee Consolidated Retirement System
TEDS	Tennessee Eligibility Determination System
TLS	Transport Layer Security
TNTAP	Tennessee Taxpayer Access Point
TPL	Third Party Liability
T-MSIS	Transformed Medicaid Statistical Information System
UAT	User Acceptance Testing
USC	United States Code
VPC	Virtual Private Cloud
VPN	Virtual Private Network
W3C	World Wide Web Consortium
WAF	Web Application Firewall
WBT	Web Based Training
WCAG	Web Content Accessibility Guidelines
WS	Web Service
XLS	Filename Extension (Microsoft Excel spreadsheet file)
XML	Extensible Markup Language

Docusign Envelope ID: 40B7BFA4-E1BB-4360-9C9C-6FA33E97F12A

SERVICE LEVEL AGREEMENTS AND LIQUIDATED DAMAGES

Located in the Procurement Library

Docusign Envelope ID: 40B7BFA4-E1BB-4360-9C9C-6FA33E97F12A

PROCUREMENT LIBRARY

Docusign Envelope ID: 40B7BFA4-E1BB-4360-9C9C-6FA33E97F12A

CONTRACT REQUIREMENTS INVENTORY

Located in the Procurement Library

Docusign Envelope ID: 40B7BFA4-E1BB-4360-9C9C-6FA33E97F12A

CONTRACT ATTACHMENT E

ATTESTATION RE PERSONNEL USED IN CONTRACT PERFORMANCE

SUBJECT CONTRACT NUMBER:	RFP 31865-00641
CONTRACTOR LEGAL ENTITY NAME:	Inspira Enterprise, Inc.
EDISON VENDOR IDENTIFICATION NUMBER:	0000285177

The Contractor, identified above, does hereby attest, certify, warrant, and assure that the Contractor shall not knowingly utilize the services of an illegal immigrant in the performance of this Contract and shall not knowingly utilize the services of any subcontractor who will utilize the services of an illegal immigrant in the performance of this Contract.

Signed by:
Amit Gandre
5100B80A4ECA44E...

CONTRACTOR SIGNATURE

NOTICE: This attestation MUST be signed by an individual empowered to contractually bind the Contractor. Attach evidence documenting the individual's authority to contractually bind the Contractor, unless the signatory is the Contractor's chief executive or president.

Amit Gandre CEO, Americas

PRINTED NAME AND TITLE OF SIGNATORY

3/7/2025

DATE OF ATTESTATION

Docusign Envelope ID: 40B7BFA4-E1BB-4360-9C9C-6FA33E97F12A

CONTRACT ATTACHMENT F

HIPAA Business Associate Agreement

THIS HIPAA BUSINESS ASSOCIATE AGREEMENT ("Agreement") is between The State of Tennessee, Division of TennCare ("TennCare" or "Covered Entity"), located at 310 Great Circle Road, Nashville, TN 37228 and INSPIRA ENTERPRISE, INC. ("Business Associate"), located at 1301 SOLANA BLVD., SUITE 2570, WESTLAKE, TEXAS 76262, including all office locations and other business locations at which Business Associate data may be used or maintained. Covered Entity and Business Associate may be referred to herein individually as "Party" or collectively as "Parties."

BACKGROUND

The Parties acknowledge that they are subject to the Privacy and Security Rules (45 C.F.R. Parts 160 and 164) promulgated by the United States Department of Health and Human Services pursuant to the Health Insurance Portability and Accountability Act of 1996 ("HIPAA"), Public Law 104-191, and as amended by the final rule modifying the HIPAA Privacy, Security, Enforcement, and Breach Notification Rules under the Health Information Technology for Economic and Clinical Health Act ("HITECH"). If Business Associate provides services to Covered Entity pursuant to one or more contractual relationships, said agreements are detailed below and hereinafter referred to as "State Contract" or "State Contracts."

LIST OF STATE CONTRACTS AFFECTED BY THIS HIPAA BUSINESS ASSOCIATE AGREEMENT:

RFP 31865-00641

In the course of performing services under the State Contract(s), Business Associate may come into contact with, use, or disclose Protected Health Information ("PHI"). Said State Contract(s) is/are hereby incorporated by reference and shall be considered part of this Agreement as if the State Contract(s) was/were fully included herein.

In accordance with the federal privacy and security rules and regulations set forth at 45 C.F.R. Part 160 and Part 164, Subparts A, C, D, and E, which require Covered Entity to have a written memorandum with each of its Business Associates, the Parties agree to establish satisfactory assurances that Business Associate will appropriately safeguard PHI that Business Associate receives from or on behalf of Covered Entity, and therefore, the Parties execute this Agreement.

In the case of any conflict, discrepancy, or ambiguity, between this Agreement and the State Contract(s), this Agreement shall govern as relating to the conflict, discrepancy, or ambiguity only. Absent any conflict, discrepancy, or ambiguity between this Agreement and the State Contract(s), the State Contract governs.

1. DEFINITIONS

Docusign Envelope ID: 40B7BFA4-E1BB-4360-9C9C-6FA33E97F12A

All capitalized terms used but not otherwise defined in this Agreement shall have the same meaning as the defined terms in 45 C.F.R. Parts 160 through 164, or other applicable law or regulation. A reference in this Agreement to the Privacy or Security Rule means the rule or section as in effect as of the date of this Agreement or as amended after the execution of this Agreement.

1.1 "Commercial Use" means obtaining PHI with the intent to sell, transfer or use it for commercial or personal gain, or malicious harm; selling to a third party for consumption, resale, or processing for resale; applying or converting data to make a profit or obtain a benefit contrary to the spirit of this Agreement, including but not limited to, presentation of data or examples of data in a presentation, conference, or meeting setting, with a goal of obtaining or gaining new business.

1.2 "Confidential Information" shall mean any non-public, confidential, or proprietary information, whether written, graphic, oral, electronic, visual or fixed in any tangible medium or expression, which is supplied by TennCare to Business Associate under this Agreement. Any information, whether written, graphic, oral, electronic, visual or fixed in any tangible medium or expression, relating to any individual enrolled in the TennCare program ("TennCare Enrollee"), or relating to individual(s) who may potentially enroll in the TennCare program, provided to or obtained through Business Associate's performance under this Agreement, shall also be treated as Confidential Information to the extent that confidential status is afforded under state and federal laws or regulations to the information provided to, or obtained through, Business Associate's performance. All Confidential Information shall not be subject to disclosure under the Tennessee Public Records Act.

1.3 "Electronic Signature(s)" means an electronic sound, symbol, or process attached to or logically associated with a record and executed or adopted by a person with the intent to sign the record.

1.4 "Marketing" shall have the meaning under 45 C.F.R. § 164.501 and shall include the act or process of promoting, selling, leasing, or licensing any TennCare information or data for profit, advantage, benefit, or similar goal, without the express written permission of TennCare.

2. OBLIGATIONS AND ACTIVITIES OF BUSINESS ASSOCIATE (PRIVACY RULE)

2.1 Compliance with the Privacy Rule. Business Associate shall fully comply with the requirements under the Privacy Rule applicable to "business associates," as that term is defined in the Privacy Rule, and not use or further disclose PHI other than as permitted or required by this Agreement, the State Contract(s), or as required by law.

2.2 HIPAA and HITECH Compliance. HITECH and its implementing regulations impose requirements on business associates with respect to privacy, security, and Breach notification. Business Associate hereby acknowledges and agrees that it is functioning as a Business Associate of Covered Entity as obligated by this Agreement and the State Contract(s). Business Associate further acknowledges that it shall comply with any applicable provisions of HIPAA and HITECH. Business Associate and Covered Entity further agree that the provisions of HIPAA and HITECH that apply to business associates, and that are required to be incorporated by reference in a business associate agreement, have been incorporated into this Agreement between Business Associate and Covered Entity. Even if a provision of HIPAA or HITECH is not specifically set forth in this Agreement, all applicable provisions of HIPAA and HITECH are incorporated into this Agreement in their entirety.

2.3 Business Management. Business Associate may use and disclose PHI for the proper management and administration of Business Associate or to carry out the legal responsibilities of Business Associate. Business Associate may provide data aggregation services relating to the Health Care Operations of TennCare, or as required by law. Business Associate is expressly prohibited from using or disclosing PHI other than as permitted by this

Docusign Envelope ID: 40B7BFA4-E1BB-4360-9C9C-6FA33E97F12A

Agreement, any associated State Contract(s), or as otherwise required by law, and is prohibited from uses or disclosures of PHI that would not be permitted if done by Covered Entity.

2.4 Privacy Safeguards and Policies. Business Associate shall use appropriate safeguards to prevent use or disclosure of PHI other than as provided for by the State Contract(s), this Agreement, or as required by law. This includes the implementation of Administrative, Physical, and Technical Safeguards to appropriately protect Covered Entity's PHI against any reasonably anticipated threats or hazards utilizing the technology commercially available to Business Associate (See also Agreement Section 3.2). Business Associate shall maintain, and provide to TennCare when requested, appropriate documentation of Business Associate's compliance with the Privacy Rule, except when Business Associate is required by TennCare policies and procedures to provide compliance documents on an established timeframe without request from TennCare. Appropriate documentation of compliance with the Privacy Rule includes, but is not limited to, Business Associate's policies and procedures, records of training, records of breaches, and sanctions of members of its Workforce.

2.5 Privacy Provisions in Business Associate Contracts. Business Associate shall require any agent, including a subcontractor, to whom it provides PHI received from, maintained, created, or received by Business Associate on behalf of Covered Entity, or that carries out any duties for Business Associate involving the use, custody, disclosure, creation of, or access to, PHI or other confidential TennCare information, to enter into a written contract that is substantially similar to this Agreement with respect to all privacy provisions. Said substantially similar written contract shall not include less stringent terms or restrictions than this Agreement with Business Associate with respect to the privacy provisions, except for Agreement Section 4.4.2, which shall only apply to Business Associate notwithstanding the requirements in this Agreement Section 2.5.

2.6 Mitigation of Harmful Effect of Violations. Business Associate agrees to mitigate, to the extent practicable, any harmful effect that is known to Business Associate of a use or disclosure of PHI by Business Associate in violation of the requirements of this Agreement. Business Associate also agrees to consult with TennCare about any mitigation efforts.

2.7 Reporting of Violations and Reasonably Suspected Violations in Use and Disclosure of PHI. Business Associate shall require its employees, agents, and subcontractors to promptly report to Business Associate immediately upon becoming aware, or upon reasonable suspicion, of any use or disclosure or reasonably suspected use or disclosure of PHI in violation of, or otherwise not provided by, this Agreement. Business Associate shall make its report to Covered Entity immediately upon becoming aware of any use or disclosure or reasonably suspected use or disclosure of PHI not provided by this Agreement, and in no case shall the Business Associate take longer than forty-eight (48) hours to report the discovery to Covered Entity. Reports shall be submitted as provided for in Agreement Section 3.5.

2.8 Breach of Unsecured Protected Health Information. As required by the Breach Notification Rule, Business Associate shall, and shall require its subcontractor(s) to, maintain systems to monitor and detect a Breach of Unsecured PHI whether in paper or electronic form.

2.8.1 Business Associate shall provide to Covered Entity notice of a Breach of Unsecured PHI or a suspected Breach of Unsecured PHI immediately upon becoming aware or upon reasonable suspicion of the Breach, and in no case later than forty-eight (48) hours after becoming aware or upon reasonable suspicion. Notice shall be submitted as provided for in Agreement Section 3.5.

2.8.2 Business Associate shall cooperate with Covered Entity by timely providing the appropriate and necessary information to Covered Entity, as reasonably anticipated or otherwise requested by Covered Entity.

Docusign Envelope ID: 40B7BFA4-E1BB-4360-9C9C-6FA33E97F12A

2.8.3 Covered Entity shall make the final determination on whether the Breach requires notification to affected individuals and whether the notification shall be made by Covered Entity or Business Associate.

2.9 Access of Individual to PHI. In the event an Individual requests access to PHI and Business Associate's participation is necessary to comply with the request, Business Associate agrees to timely respond as further outlined below.

2.9.1 Requests Submitted to Covered Entity that Require Business Associate's Participation. Covered Entity shall forward to Business Associate in a timely manner any Individual's request for access to or a copy of the Individual's PHI, in any form the Individual chooses if the PHI is readily producible in that format.

2.9.2 Requests Submitted to Business Associate.

(a) If Business Associate receives PHI from Covered Entity in a Designated Record Set, Business Associate agrees to provide access to PHI in a Designated Record Set to Covered Entity to meet the requirements of 45 C.F.R. § 164.524.
(b) If Business Associate receives a request from an Individual for a copy of the Individual's PHI, and the PHI is in the sole possession of Business Associate, Business Associate will provide the requested copy to the Individual as specified in 2.9.3(a). If Business Associate provides copies of PHI to the Individual, it may charge a reasonable fee for the copies as permitted by applicable regulations. Business Associate is permitted to send to an Individual or Individual's designee unencrypted emails including Electronic PHI if the Individual requests it, provided Business Associate has advised the Individual of the associated risk and the Individual still chooses to receive the message by unencrypted email.
(c) If Business Associate receives a request for PHI not in its possession and in the possession of Covered Entity or receives a request to exercise other Individual rights as set forth in the Privacy Rule, Business Associate shall promptly forward the request to Covered Entity. Business Associate shall then assist Covered Entity, as necessary, in responding to the request timely.

2.9.3 Timeframes for Response.

(a) The Parties understand that if either Party receives a request for access to or copies of PHI from an Individual that the Party may complete with only its own onsite information, the time for providing a response to the Individual shall be no more than thirty (30) days, or a timeframe otherwise in compliance with 45 C.F.R. § 164.524. Business Associate shall also notify Covered Entity upon completion of the request.
(b) If Covered Entity receives a request from an Individual for access to or copies of PHI, and requires information from Business Associate in addition to Covered Entity's onsite information to fulfill the request, Business Associate shall have no more than fifteen (15) days, from the date of Covered Entity's notice, to provide access or deliver such information to Covered Entity so that Covered Entity may timely respond to the Individual within the thirty (30) day requirement of 45 C.F.R. § 164.524.
(c) If the Party responsible for responding to the Individual's request for access to or copies of PHI is unable to complete the response to the request in the required timeframe, the responsible Party shall provide the Individual, or Individual's designee, with a written statement of the reasons for the delay and the date by which the Party will complete its action on the request. The Party may extend the response one (1) time for no more than thirty (30) additional days.

2.10 Individual's Request to Amend PHI. If Business Associate receives PHI from Covered Entity in a Designated Record Set and an Individual requests to amend PHI, Business Associate agrees to make any amendments to PHI in a Designated Record Set that Covered Entity directs or agrees to pursuant to 45 C.F.R. § 164.526. Business Associate shall make the amendment promptly in the time and manner designated by Covered Entity and shall notify

Docusign Envelope ID: 40B7BFA4-E1BB-4360-9C9C-6FA33E97F12A

Covered Entity upon completion. Business Associate shall have thirty (30) days from Covered Entity's notice to complete the amendment to the Individual's PHI.

2.11 Recording of Designated Disclosures of PHI. Business Associate shall document any and all disclosure(s) of PHI by Business Associate or its agents, including information related to such disclosures, as would be required for Covered Entity to respond to a request by an Individual for an accounting of disclosures of PHI in accordance with 45 C.F.R. § 164.528.

2.12 Accounting for Disclosures of PHI. In the timeframe and manner designated by Covered Entity, Business Associate agrees to provide to Covered Entity, or an Individual or Individual's designee, information collected in accordance with this Agreement to enable Covered Entity to respond to a request from an Individual for an accounting of disclosures of PHI in accordance with 45 C.F.R. § 164.528. Covered Entity shall forward the Individual's request requiring the participation of Business Associate to Business Associate in a timely manner, after which Business Associate shall provide the accounting of disclosures of PHI to Covered Entity as follows:

(a) If Covered Entity directs Business Associate to provide an accounting of disclosures of the Individual's PHI directly to the Individual, Business Associate shall have sixty (60) days from the date of the Individual's request to provide access or deliver such information to the Individual or Individual's designee. Covered Entity shall provide notice to Business Associate in time to allow Business Associate a minimum of thirty (30) days to timely complete the Individual's request.

(b) If Covered Entity elects to provide the accounting to the Individual, Business Associate shall have thirty (30) days from the date of Covered Entity's notice requesting information for the Accounting to Covered Entity so that Covered Entity may timely respond to the Individual within the sixty (60) day period.

(c) If either Party is unable to complete the response to the request in the timeframes provided in 2.12(a) or 2.12(b), the Party to complete the response shall notify the Individual with a written statement of the reasons for the delay and the date by which the Party will complete its action on the request. The Parties may extend the response to Individual or Individual's designee one (1) time for no more than thirty (30) additional days.

(d) The accounting of disclosures shall include at least the following information:

(1) date of the disclosure;
(2) name of the third party to whom the PHI was disclosed,
(3) if known, the address of the third party;
(4) brief description of the disclosed information; and
(5) brief explanation of the purpose and basis for such disclosure.

(e) The Parties shall provide one (1) accounting in any twelve (12) months to the Individual or Individual's designee without charge. The Parties may charge a reasonable, cost-based fee, for each subsequent request for an accounting by or regarding the same Individual if Individual or Individual Designee is provided notice and the opportunity to modify the request. Such charges shall not exceed any applicable State statutes or rules.

2.13 Minimum Necessary. Business Associate shall use reasonable efforts to limit any use, disclosure, or request for use or disclosure, of PHI to the minimum amount necessary to accomplish the intended purpose of the use, disclosure, or request in accordance with the requirements of the Privacy Rule. Reasonable efforts may include, but are not limited to, application of recognized industry standards on data minimization and retention privacy controls.

2.13.1 Business Associate represents to Covered Entity that all Business Associate's uses and disclosures of, or requests for, PHI shall be the minimum necessary in accordance with the Privacy Rule requirements.

Docusign Envelope ID: 40B7BFA4-E1BB-4360-9C9C-6FA33E97F12A

2.13.2 Covered Entity may, pursuant to the Privacy Rule, reasonably rely on any requested disclosure from Business Associate as the minimum necessary for the stated purpose.

2.13.3 Business Associate shall adequately and properly maintain all PHI received from, or created or received on behalf of, Covered Entity. Properly maintaining PHI shall include, but is not limited to, use of reasonable efforts to timely deidentify or destroy PHI Business Associate receives that is irrelevant or unnecessary for the purposes of this Agreement and any State Contract(s).

2.14 Privacy Compliance Review Upon Request. Business Associate agrees to provide its internal practices, books and records, and policies and procedures, relating to the use and disclosure of PHI received from, or created or received by Business Associate on behalf of Covered Entity, to Covered Entity or the Secretary of the United States Department of Health in Human Services or the Secretary's designee, in a timeframe and manner designated by the requester for purposes of determining Covered Entity's or Business Associate's compliance with the Privacy Rule.

2.15 Cooperation in Privacy Compliance. Business Associate agrees to fully cooperate in good faith and to assist Covered Entity in complying with the requirements of the Privacy Rule.

3. OBLIGATIONS AND ACTIVITIES OF BUSINESS ASSOCIATE (SECURITY RULE)

3.1 Compliance with Security Rule. Business Associate shall fully comply with the requirements of the Security Rule applicable to "Business Associates", as the term is defined in the Security Rule. In the case of any conflict, ambiguity, or discrepancies in language between this Agreement and the State Contract(s), this Agreement governs as to the applicable conflict, ambiguity, or discrepancies in language. If no conflict, ambiguity, or discrepancy in language exists, the State Contract governs.

3.2 Security Safeguards and Policies. Business Associates shall implement and maintain information security policies that comply with the HIPAA Security Rule. Business Associate shall implement Administrative, Physical, and Technical Safeguards that reasonably and appropriately protect the confidentiality, integrity, and availability of the Electronic PHI that it creates, receives, maintains, or transmits on behalf of Covered Entity as required by the Security Rule. This includes specifically, but is not limited to, the utilization of technology commercially available to Business Associate to protect Covered Entity's PHI against any reasonably anticipated threats or hazards. Business Associate understands that it has an affirmative duty to perform a regular review or assessment of security risks, conduct active risk management, and supply best efforts to assure that only authorized persons, entities, programs, or applications, and devices access its computing systems and information storage, and that only authorized transactions are allowed. Business Associate will maintain appropriate documentation of its compliance with the Security Rule.

3.3 Security Provisions in Business Associate Contracts. Business Associate shall ensure that any agent or subcontractor to whom Business Associate provides Electronic PHI received from, maintained, or created for Covered Entity, or that carries out any duties for Business Associate involving the use, custody, disclosure, creation of, or access to PHI supplied by Covered Entity, shall execute a contract with Business Associate (or the appropriate equivalent if the agent is a government entity) that is substantially similar to this Agreement with no less stringent restrictions and conditions as the security provisions are in this Agreement, except for the provision in Section 4.4.2.

3.4 Reporting of Security Incidents. Business Associate shall track all Security Incidents as defined and as required by HIPAA and shall periodically report a summary of the Security Incidents as may be requested by Covered Entity.

Docusign Envelope ID: 40B7BFA4-E1BB-4360-9C9C-6FA33E97F12A

For the purposes of reporting, Covered Entity shall not consider as Security Incidents, external activities (e.g., port enumeration) typically associated with the "footprinting" of a computing environment as long as such activities have only identified, but not compromised, the logical network perimeter including but not limited to externally facing firewalls and web servers. Business Associate shall reasonably use its own vulnerability assessment of damage potential and monitoring to define levels of Security Incidents and responses for Business Associate's operations. However, Business Associate shall expediently notify Covered Entity's Privacy Officer of any related Security Incident immediately upon becoming aware or upon reasonable suspicion of any unauthorized acquisition, including but not limited to, the use, disclosure, modification, or destruction of PHI, by an employee or otherwise authorized or unauthorized user of its system.

3.4.1 Business Associate identifies the following key contact person(s) for all matters relating to this Agreement:

Amit Gandre - amit.gandre@inspiraenterprise.com

Vishal Jain - vishal.jain@inspiraenterprise.com

Inspira Legal - Inspira.Legal@inspiraenterprise.com

Business Associate shall notify Covered Entity in writing of any change in the key contact(s) during the term of this Agreement within ten (10) business days of the change.

3.5 TennCare Contact for Privacy and Security Incident Notice. Notification for the purposes of Agreement Sections 2.7, 2.8 and 3.4 shall be made in writing immediately upon becoming aware, or upon reasonable suspicion, of the event. Written notice may be submitted via TennCare's privacy incident reporting form if accessible to Business Associate, email, certified mail, or overnight parcel to:

Division of TennCare **Attention**: Privacy Office
310 Great Circle Rd.
Nashville, Tennessee 37243
Phone: (866) 797-9469
Email: Privacy.Tenncare@tn.gov

3.6 Security Compliance Review upon Request. Business Associate shall provide its internal practices, books, records, and policies and procedures relating to the security of Electronic PHI received from Covered Entity, or created or received by Business Associate on behalf of Covered Entity, to Covered Entity or the Secretary of the United States Department of Health in Human Services or the Secretary's designee, in a time and manner designated by the requester for purposes of determining Covered Entity's or Business Associate's compliance with the Security Rule.

3.7 Cooperation in Security Compliance. Business Associate shall fully cooperate in good faith to assist Covered Entity in complying with the requirements of the Security Rule.

3.8 Refraining from intimidation or retaliation. Covered Entity or Business Associate may not threaten, intimidate, coerce, harass, discriminate against, or take any other retaliatory action against any Individual or other person for: (a) Filing of a complaint under 45 C.F.R. § 160.306; (b) testifying, assisting, or participating in an investigation, compliance review, proceeding, or hearing; or (c) opposing any act or practice made unlawful, provided the Individual or person has a good faith belief that the practice opposed is unlawful, and the manner of opposition is

Docusign Envelope ID: 40B7BFA4-E1BB-4360-9C9C-6FA33E97F12A

reasonable and does not involve a disclosure of PHI in violation of HIPAA.

4. USES AND DISCLOSURES BY BUSINESS ASSOCIATE

4.1 Use and Disclosure of PHI for Operations on Behalf of Covered Entity. Except as otherwise limited in this Agreement, Business Associate may use or disclose PHI to perform Treatment, Payment, or Health Care Operations for or on behalf of Covered Entity as specified in the State Contract(s), provided that such use or disclosure would not violate the Privacy and Security Rule if done by Covered Entity.

4.2 Business Associate Uses of PHI. Except as otherwise limited in this Agreement, Business Associate may disclose PHI as required for the proper management and administration of Business Associate or to carry out the legal responsibilities of Business Associate, provided that the disclosures are required by law and are also permitted by this Agreement and the State Contract(s). Nothing in this Agreement Section 4.2 permits, or should be construed as permitting, the Business Associate to use PHI for Marketing or Commercial Use.

4.3 Third Party Disclosure Confidentiality. If Business Associate discloses any PHI to a third party for a purpose permitted under 4.2, Business Associate agrees that it shall enter into a written agreement with such third party requiring the third party to: (a) maintain the confidentiality, integrity, and availability of PHI and not to use or further disclose PHI except as required by law or for the purpose for which it was disclosed; and (b) notify Business Associate of any instances where third party becomes aware that the confidentiality, integrity, and/or availability of the PHI is Breached.

4.4 Prohibited Uses and Disclosures. Nothing in this Agreement shall authorize Business Associate to share, use or disclose PHI via any form or medium for the purposes outlined in Agreement Subsections 4.4.1 through 4.4.4.

4.4.1 Marketing and Commercial Use. Business Associate shall not share, use, or disclose PHI for the purposes of selling, Marketing, or any Commercial Use, or for any purpose construed by Covered Entity as the selling, Marketing, or Commercial Use of TennCare Enrollee personal or financial information with affiliates or otherwise, even if such sharing would be permitted by federal or state laws.

4.4.2 Offshore Disclosure. Business Associate shall not share, use, or disclose PHI with any third party beyond the boundaries and jurisdiction of the United States without express written authorization from Covered Entity.

4.4.3 Genetic Information for Underwriting Purposes. Business Associate shall not use or disclose PHI that is Genetic Information for underwriting purposes.

4.4.4 Other Uses and Disclosures Strictly Prohibited. Nothing in this Agreement shall permit Business Associate to share PHI with Business Associate's affiliates, contractors, subcontractors, or other third parties, except for the purposes of the State Contract(s) identified in the "LIST OF STATE CONTRACTS AFFECTED BY THIS HIPAA BUSINESS ASSOCIATE AGREEMENT" on page one (1) of this Agreement.

4.5 Covered Entity Authorization for Additional Uses. Any use of PHI or other Confidential Information by Business Associate, its subcontractors, its affiliates, or Contractors, other than the use permitted for the purposes of this Agreement, shall require express written authorization by Covered Entity, and a Business Associate Agreement or amendment as necessary. Activities which are prohibited include, but are not limited to, Marketing, sharing for Commercial Use, or any purpose construed by Covered Entity as Marketing or Commercial use of TennCare Enrollee personal or financial information with affiliates, even if such sharing would be permitted by federal or state laws.

Docusign Envelope ID: 40B7BFA4-E1BB-4360-9C9C-6FA33E97F12A

4.6 Data Use Agreement - Use and Disclosure of Limited Data Set. Business Associate may use and disclose a Limited Data Set that Business Associate creates for Research, public health activity, or Health Care Operations, provided Business Associate complies with the obligations in Agreement Section 3.2 and this Agreement. Business Associate may not make such use and disclosure of the Limited Data Set after any cancellation, termination, expiration, or other conclusion of this Agreement.

4.7 Limitation on Permitted Uses and Disclosures. Business Associate will limit the uses and disclosures of the Limited Data Set to the following: Research, public health activity, or Health Care Operations, to the extent such activities are related to covered functions. Covered functions for purposes of this Agreement Section 4.7 shall include business planning and development, such as: conducting cost-management and planning-related analysis related to managing and operating Business Associate's functions; formulary development and administration; development and improvement of methods of payment or coverage policies; and customer service, including the provision of data analysis for policy holders, plan sponsors, or other customers to the extent such activities are related to covered functions. The listed covered functions shall only be permitted if PHI is not disclosed, and disclosure is not prohibited pursuant to any other provisions in this Agreement.

5. OBLIGATIONS OF COVERED ENTITY

5.1 Notice of Privacy Practices. Covered Entity shall provide Business Associate with the Covered Entity's notice of Privacy Practices in accordance with 45 C.F.R. § 164.520, as well as any changes to the notice of Privacy Practices. Notice may be provided via publication on TennCare's website.

5.2 Notice of Changes in Individual's Authorization for Access to PHI. Covered Entity shall provide Business Associate with any changes in, or revocation of, permission by an Individual to use or disclose PHI, if such changes affect Business Associate's permitted or required uses.

5.3 Notice of Restriction in Individual's Access to PHI. Covered Entity shall notify Business Associate of any restriction to the use or disclosure of PHI that Covered Entity has agreed to in accordance with 45 C.F.R. § 164.522, to the extent that such restriction may affect Business Associate's use of PHI.

5.4 Reciprocity for Requests Received by Business Associate. The Parties agree that Agreement Sections 5.2 through 5.3 are reciprocal, to the extent Business Associate is notified or receives an inquiry from any Individual within Covered Entity's covered population.

6. TERM AND TERMINATION

6.1 Term. This Agreement shall be effective on the date of the last signatory, or on the signature date if all Parties sign on the same day, and shall terminate when all PHI, regardless of form, provided by Covered Entity to Business Associate, or created or received by Business Associate on behalf of Covered Entity, is destroyed or returned to Covered Entity, or if the Parties mutually agree in writing that it is unfeasible to return or destroy PHI, Agreement Subsection 6.3.5 below applies.

6.2 Termination for Cause. This Agreement authorizes, and Business Associate acknowledges and agrees, Covered Entity shall have the right to terminate this Agreement and any State Contracts in the event Business Associate fails to comply with or violates a material provision of this Agreement and any provision of the Privacy and Security Rules. Nothing in Agreement Section 6.2 limits the State's ability to terminate the State Contract as permissible

Docusign Envelope ID: 40B7BFA4-E1BB-4360-9C9C-6FA33E97F12A

under the State Contract.

6.2.1 Upon Covered Entity's knowledge of a breach by Business Associate of the terms of this Agreement or any State Contract (s), Covered Entity shall either:

(a) Provide notice of breach and an opportunity for Business Associate to reasonably and promptly cure the breach or end the violation. If Business Associate does not cure the breach or end the violation within the reasonable time following notice, as specified by Covered Entity, Covered Entity shall terminate this BAA; or

(b) Immediately terminate this BAA if Business Associate has breached a material term of this BAA and cure is not possible.

6.3 Effect of Termination. Upon termination of this Agreement for any reason, except as provided in Agreement Subsections 6.3.2 and 6.3.5, Business Associate shall at its own expense either return and/or destroy all PHI and other Confidential Information received from Covered Entity or created or received by Business Associate on behalf of Covered Entity. This provision applies to all Confidential Information regardless of form, including but not limited to, electronic or paper format. This provision shall also apply to PHI and other Confidential Information in the possession of subcontractors or agents of Business Associate.

6.3.1 Business Associate shall consult with Covered Entity as necessary to ensure an appropriate means of return or destruction of PHI and Confidential Information and shall notify Covered Entity in writing when such destruction is complete. If PHI or Confidential Information is to be returned, the Parties shall document when all information has been received by Covered Entity.

6.3.2 Agreement Section 6.3 and its Subsections shall not prohibit the retention of a single separate, archived file of the PHI and other confidential TennCare information by Business Associate if the method of such archiving reasonably protects the continued privacy and security of such information and Business Associate obtains written approval at the time of archival from Covered Entity.

Otherwise, neither Business Associate nor its subcontractors and agents shall retain copies of TennCare Confidential Information including enrollee PHI, except as provided herein in Agreement Subsection 6.3.5.

6.3.3 The Parties agree to anticipate the return or the destruction of PHI and other Confidential Information and understand that removal of the Confidential Information from Business Associate's information system(s) and premises will be expected in almost all circumstances. Business Associate shall notify Covered Entity whether it intends to return or destroy the PHI or Confidential Information with additional detail as requested by Covered Entity. In the event Business Associate determines that returning or destroying the PHI and other Confidential Information received by or created for Covered Entity at the end or other termination of the State Contract(s) is not feasible, Business Associate shall provide to Covered Entity notification of the conditions that make return or destruction unfeasible.

6.3.4 Except for Business Associate agreements in effect prior to April 21, 2005, for the renewal or amendment of those same agreements, or for other unavoidable circumstances, the Parties contemplate that PHI and other Confidential Information of Covered Entity shall not be merged or aggregated with data from sources unrelated to that agreement, or Business Associate's other business data, including for purposes of data backup and disaster recovery, until the Parties identify the means of return or destruction of the TennCare data or other Confidential Information of Covered Entity at the conclusion of any State Contract(s), or otherwise make an express alternate agreement consistent with the provisions of Agreement Section 6.3

Docusign Envelope ID: 40B7BFA4-E1BB-4360-9C9C-6FA33E97F12A

and its Subsections.

6.3.5 Upon written mutual agreement of the Parties that the return or destruction of PHI or Confidential Information is unfeasible and upon express agreement as to the means of continued protection of the data, Business Associate shall extend the protections of this Agreement to such PHI and limit further uses and disclosures of such PHI to those purposes that make the return or destruction unfeasible, for so long as Business Associate maintains such PHI.

7. MISCELLANEOUS

7.1 Amendment. The Parties agree to amend this Agreement from time to time as is necessary for Covered Entity or Business Associate to comply with the requirements of the Privacy and Security Rules and the Health Insurance Portability and Accountability Act, Public Law 104-191. Business Associate and Covered Entity shall comply with any amendment to the Privacy and Security Rules, the Health Insurance Portability and Accountability Act, Public Law 104-191, and related regulations upon the effective date of such amendment, regardless of whether this Agreement has been formally amended, including, but not limited to, changes required by the American Recovery and Reinvestment Act of 2009, Public Law 111-5.

7.2 Survival. The respective rights and obligations of Business Associate under applicable confidentiality provisions and Agreement Sections 4 and its Subsections, and 6.3 and its Subsections, shall survive the termination or expiration of this Agreement.

7.3 Interpretation. Any ambiguity in this Agreement shall be resolved in favor of a meaning that permits Covered Entity and Business Associate to comply with the Privacy and Security Rules.

7.4 Headings. Paragraph Headings used in this Agreement are for the convenience of the Parties and shall have no legal meaning in the interpretation of the Agreement.

7.5 Notices and Communications. Except as specified in Agreement Section 3.5, all instructions, notices, consents, demands, or other communications required or contemplated by this Agreement shall be in writing and shall be delivered by electronic mail, hand, by facsimile transmission, by overnight courier service, or by first class mail, postage prepaid, addressed to the respective party at the appropriate facsimile number or address as set forth below, or to such other party, facsimile number, or address as may be hereafter specified by written notice. (For purposes of Agreement Section 7.6, effective notice to "Respective Party" is not dependent on whether the person named below remains employed by such Party). The Parties agree to use their best efforts to immediately notify the other Party of changes in address, telephone number, and fax numbers and to promptly supplement this Agreement as necessary with corrected information.

Notifications relative to Agreement Sections 2.7, 2.8 and, 3.4 of this Agreement need only be reported to the Privacy Office pursuant to Agreement Section 3.5.

COVERED ENTITY:	BUSINESS ASSOCIATE:
Stephen Smith, Director Division of TennCare 310 Great Circle Rd.	Amit Gandre CEO, Americas 1301 SOLANA BLVD., SUITE 2570

Docusign Envelope ID: 40B7BFA4-E1BB-4360-9C9C-6FA33E97F12A

Nashville, TN 37243
Fax: (615) 253-5607

WESTLAKE, TEXAS 76262
(254) 467-7472

All instructions, notices, consents, demands, or other communications shall be considered effectively given as follows: on the date of hand delivery; on the date specified for overnight courier service delivery; as of three (3) business days after the date of mailing by first class mail postage prepaid; on the day the facsimile transmission is received mechanically by the facsimile machine at the receiving location and receipt is verbally confirmed by the sender; or via electronic submission as approved or as directed by TennCare.

7.6 Transmission of PHI or Other Confidential Information. Regardless of the transmittal methods permitted above, Covered Entity and Business Associate agree that all deliverables set forth in this Agreement that are required to be in the form of data transfers shall be transmitted between Covered Entity and Business Associate via the data transfer method specified in advance by Covered Entity. This may include, but shall not be limited to, transfer through Covered Entity's SFTP system. Failure by Business Associate to transmit such deliverables in the manner specified by Covered Entity may, at the option of Covered Entity, result in liquidated damages as set forth in one (1) or more of the State Contracts between Covered Entity and Business Associate listed above. All such deliverables shall be considered effectively submitted upon receipt or recipient confirmation as may be required.

7.7 Strict Compliance. No failure by any Party to insist on strict compliance with any term or provision of this Agreement, to exercise any option, to enforce any right, or to seek any remedy upon any default of any other Party shall affect, or constitute a waiver of, any Party's right to insist on strict compliance, exercise that option, enforce that right, or seek that remedy with respect to the default or any prior, contemporaneous, or subsequent default. No custom or practice of the Parties at variance with any provision of this Agreement shall affect, or constitute a waiver of, any Party's right to demand strict compliance with all provisions of this Agreement.

7.8 Severability. With respect to any provision of this Agreement finally determined by a court of competent jurisdiction to be unenforceable, such court shall have jurisdiction to reform such provision so that it is enforceable to the maximum extent permitted by applicable law, and the Parties shall abide by such court's determination. If any provision of this Agreement cannot be reformed, such provision shall be deemed to be severed from this Agreement and all other provisions of this Agreement shall remain in full force and effect.

7.9 Governing Law. This Agreement shall be governed by and construed in accordance with the laws of the State of Tennessee except to the extent that Tennessee law has been pre-empted by HIPAA and HITECH and without giving effect to principles of conflicts of law.

7.10 Compensation. There shall be no remuneration for performance under this Agreement except as specifically provided by, in, and through, existing administrative requirements of Tennessee State government and State Contract(s) referenced herein.

7.11 Validity of Execution. Unless otherwise agreed, the Parties may conduct the execution of this Business Associate Agreement transaction by electronic means. The parties may agree that an electronic record of the Agreement containing Electronic Signatures is valid as an executed Agreement.

IN WITNESS WHEREOF, the Parties execute this Agreement to be valid and enforceable from the latest dated signature set out below or on the date of signatures if both Parties sign on the same date:

Docusign Envelope ID: 40B7BFA4-E1BB-4360-9C9C-6FA33E97F12A

F.DIVISION OF TENNCARE

By: Stephen Smith /ZS

Stephen Smith, Director

Date: 3/25/2025

Division of TennCare
310 Great Circle Road
Nashville, TN 37243
Fax: (615) 253-5607

BUSINESS ASSOCIATE

Signed by:
By: Amit Gandre
5100BB0A4ECA44E...

Amit Gandre

CEO, Americas

Date: 3/7/2025

INSPIRA ENTERPRISE, INC.
1301 SOLANA BLVD., SUITE 2570,
WESTLAKE, TEXAS 76262