STATE OF VERMONT
CONTRACT AMENDMENT

It is hereby agreed by and between the State of Vermont, Department of Vermont Health Access (the "State") and OptumInsight, Inc., with a principal place of business in Eden Prairie, Minnesota, (the "Contractor") that the contract between them originally dated as of August 15, 2016, Contract #31750, as amended to date, (the "Contract") is hereby amended effective August 14, 2021 (Amendment No. 5) as follows:

I. **Maximum Amount.** The maximum amount payable under the Contract, wherever such reference appears in the Contract, shall be changed from $68,970,223.00 to $95,793,610.00, representing an increase of $26,823,387.00.

II. **Contract Term.** The Contract end date, wherever such reference appears in the Contract, shall be changed from August 14, 2021 to August 14, 2023. The State and Contractor have the option of renewing this Contract, for up to one (1) additional one (1) year extension as mutually agreed. If either party declines to extend the Contract for the one-year extension period, they shall provide the other party not less than 12 months' advance written notice.

III. **Attachments:** The list of attachments in Section 8 of the Contract originally appearing on Page 1 of the base agreement is hereby deleted and replaced as set forth below:

Attachment A – Specifications of Work to Be Performed
- Exhibit 1 – State Requirements and Contractor's Responsibilities listed by Service
- Exhibit 2 – Service Level Agreements and Service Level Credits
- Exhibit 3 – Security Policies
- Exhibit 4 – Deliverable Best Practices
- Exhibit 5 – Standard Form Template Quality Assurance Surveillance Plan (QASP)
- Exhibit 6 – Informational Memorandum
- Exhibit 7 – QASP for Section 26 Premium Processing Development

Attachment B – Payment Provisions
Attachment C – State Standard Provisions for Contracts and Grants
Attachment D – Other Terms and Conditions
Attachment E – Business Associate Agreement
Attachment F – AHS' Customary Contract Provisions
Attachment G – Modifications of Customary Provisions of Attachment F
Appendix I – Subcontractor Approval Form

IV. **Order of Precedence:** The Order of Precedence list in Section 9 originally appearing on Page 1 of the base agreement is hereby deleted and replaced as set forth below to include the addition of Attachment F:

Any ambiguity, conflict, or inconsistency in the Contract Documents shall be resolved according to the following order of precedence:

1. Standard Contract Pages 1-2
2. Attachment D
3. Attachment C
4. Attachment A
5. Attachment B
6. Attachment E
7. Attachment G
8. Attachment F
9. Other Attachments (if applicable)

V. **Attachment A, Specifications of Work to be Performed.** The scope of services is hereby deleted in its entirety and replaced as set forth in Attachment A to this Amendment.

VI. **Exhibits to Attachment A.** All Exhibits to Attachment A are hereby deleted and replaced with the Exhibits 1-7 as set forth in this Amendment.

VII. **Attachment B, Payment Provisions.** The payment provisions are hereby deleted in their entirety and replaced as set forth in Attachment B to this Amendment.

VIII. **Attachment D, Other Terms and Conditions.** By deleting all references in Attachment D to a "Business Partner Agreement" and replacing with "Business Associate Agreement".

IX. **Attachment F, Agency of Human Services' Customary Contract Provisions.** Attachment F is hereby added to this Contract.

X. **Attachment G, Modifications of Customary Provisions of Attachment F.** Attachment G is hereby added to this Contract.

Taxes Due to the State. Contractor further certifies under the pains and penalties of perjury that, as of the date this contract amendment is signed, the Contractor is in good standing with respect to, or in full compliance with a plan to pay, any and all taxes due the State of Vermont.

Child Support (Applicable to natural persons only; not applicable to corporations, partnerships or LLCs). Contractor is under no obligation to pay child support or is in good standing with respect to or in full compliance with a plan to pay any and all child support payable under a support order as of the date of this amendment.

Certification Regarding Suspension or Debarment. Contractor certifies under the pains and penalties of perjury that, as of the date this contract amendment is signed, neither Contractor nor Contractor's principals (officers, directors, owners, or partners) are presently debarred, suspended, proposed for debarment, declared ineligible or excluded from participation in federal programs, or programs supported in whole or in part by federal funds.

Contractor further certifies under pains and penalties of perjury that, as of the date that this contract amendment is signed, Contractor is not presently debarred, suspended, nor named on the State's debarment list at: http://bgs.vermont.gov/purchasing-contracting/debarment.

SOV Cybersecurity Standard 19-01. All products and service provided to or for the use of the State under this Contract shall be in compliance with State of Vermont Cybersecurity Standard 19-01 and Cybersecurity Standard 19-01 Update dated February 19, 2019, which Contractor acknowledges have been provided to it, and are available on-line at the following URL: https://digitalservices.vermont.gov/cybersecurity/cybersecurity-standards-and-directives.

This document consists of 131 pages. Except as modified by this Amendment No. 5, all provisions of the Contract remain in full force and effect.

The signatures of the undersigned indicate that each has read and agrees to be bound by this Amendment No.5 to the Contract.

STATE OF VERMONT
DEPARTMENT OF VERMONT HEALTH ACCESS

E-SIGNED by Adaline Strumolo
on 2021-08-25 14:15:36 GMT August 25, 2021

Adaline Strumolo Date
NOB 1 South
280 State Drive
Waterbury, VT 05671-1010
Phone: 802-503-7482
Email: Adaline.Strumolo@vermont.gov

CONTRACTOR
OPTUMINSIGHT, INC.

E-SIGNED by Paul Miller
on 2021-08-25 13:31:08 GMT August 25, 2021

Paul M. Miller, Vice President Finance Date
Optum Corporate Finance
11000 Optum Circle
Eden Prairie, MN 55344
Phone: 952-205-6089
Email: paul.m.miller@optum.com

ATTACHMENT A
SPECIFICATIONS OF WORK TO BE PERFORMED

1. THE CONTACTS FOR THIS CONTRACT ARE AS FOLLOWS:

	State Fiscal Manager	**Authorized State Representative**	**For the Contractor**
Name:	Meaghan Kelley	Darin Prail	Scott Cerreta
Phone:	(802) 241-0393	(802) 338-5719	(802) 654-0206
E-Mail:	Meaghan.Kelley@vermont.gov	Darin.Prail@vermont.gov	Scott.Cerreta@optum.com
	DVHA Contract Owner		
Name:	Molly Sweeney		
Phone:	(802) 798-2240		
E-Mail:	Molly.Sweeney@vermont.gov		

2. NOTICES TO THE PARTIES UNDER THIS CONTRACT

To the extent notices are made under this Contract, the parties agree that such notices shall only be effective if sent to the following persons as representative of the parties:

	STATE	CONTRACTOR/GRANTEE
Name	Office of General Counsel	Senior Associate General Counsel
Address	NOB 1 South, 280 State Drive Waterbury, VT 05671-1010	11000 Optum Circle, MN001-1-1376C Eden Prairie, MN 55344 USA
Email	ahs.dvhalegal@vermont.gov	aimee.blatz@optum.com

The parties agree that notices may be sent by electronic mail except for the following notices which must be sent by United States Postal Service certified mail: termination of Contract, damage claims, breach notifications and alteration of this paragraph.

3. DVHA MONITORING OF CONTRACT

The parties agree that the Authorized State Representative, or his designee, is solely responsible for the review of invoices presented by the Contractor.

4. SUBCONTRACTOR REQUIREMENTS

The State acknowledges and understands that Contractor has contracts with subcontractors that may be used in support of this Contract. Per Attachment C, Section 19, if the Contractor desires to subcontract work under this Contract, the Contractor must first fill out and submit the Subcontractor Compliance Form (Appendix I – Required Forms) in order to seek approval from the State prior to signing an agreement with a third party. Upon receipt of the Subcontractor Compliance Form, the State shall review and respond within five (5) business days. A fillable PDF version of this Subcontractor Compliance Form is available upon request from the State Business Office. Under no circumstance shall the Contractor enter into a sub-agreement without prior authorization from the State. The Contractor shall submit the Subcontractor Compliance Form to the Fiscal Manager set forth above. Upon request by State, Contractor shall deliver a copy of all applicable subcontractor contracts to the State for review; provided, however, subject to applicable law, the State shall treat such subcontracts as Contractor Confidential Information, shared with only those State employees who have a need to know and solely for the purpose of confirming that the protections described in this Contract as applicable to the subcontractor's scope of work are addressed.

5. PURPOSE

The subject matter of this Contract is services for the ongoing Information Technology Maintenance and Operations (M&O) of the State of Vermont's Vermont Health Connect (VHC) Business Applications, Health and Human Services Enterprise Platform (HSEP) and non-recurring work required to transition to a new IT Service management (ITSM) software platform (together, the "Core M&O Services"), and the creation of certain documentation, including M&O deliverables as set forth in Attachment A, Section 6.4 Table A, reports as set forth in Section 6.4 Table B, and transition deliverables as set forth in Section 6.4 Table C (collectively, "Deliverables"). The Core M&O Services and the Deliverables shall be referred to together herein as "HSEP M&O Services."

6. SCOPE OF HSEP M&O SERVICES

Contractor shall provide and perform the HSEP M&O Services described herein in accordance with, and subject to, the terms and conditions set forth in this Contract.

The HSEP M&O Services described below are for the maintenance, operation and continual improvement of State's HSEP Managed Applications, related business processes and IT support processes.

a) Managed Applications and Core M&O Services
   - HSEP M&O
   - Business Component M&O
   - ITSM
   - Application Lifecycle Management (ALM) Software
   - Root Cause Analysis
b) M&O Deliverables and Reports
c) Contractor's Management Team and Governance Activities
d) Transition Services
e) Discretionary Services

For the Managed Applications listed below in Section 6.1.1, Table 1 - Managed Applications, Contractor will provide a range of services which are enumerated in Section 6.1.2, Table 2 – Core M&O Services in Scope, and set forth in greater detail in Exhibit 1, Contractor's Responsibilities by Functional Area, to this Attachment A.

The service level requirements related to Contractor's provision of HSEP M&O Services are set forth in Exhibit 2, Service Level Agreement, to this Attachment A.

6.1 Managed Applications

6.1.1 The table below refers to those applications which are business components of the HSEP that Contractor shall support pursuant to this Contract.

Table 1 – In-Scope Managed Applications, including business components ("Managed Applications")

		HSEP Managed Applications
1.		Notification Engine
2.		Access Integration
3.		Enterprise Content Management
4.		Rules Engine (OPA)
5.		Identity and Access Management (OAM Suite)
6.		Existing Integrations and interfaces between HSEP and External Systems
7.		Web Analytics
8.		Portal (Liferay)
9.		Business Intelligence (OBIEE)
10.		Workflow Management
11.		Database Services
12.		Siebel (Case Management)
13.		SOA Suite (ESB, Registry, Repository, etc.)

All of the Managed Applications have elements or components currently installed which are intended to be used or shared by multiple HSEP tenants.

6.1.2 Core M&O Services in Scope: Contractor shall provide Core M&O Services in the following categories as they solely pertain to the Managed Applications in Table 1. Each of Core M&O Services in Scope in Table 2 below are defined in Exhibit 1 to this Attachment A in more detail, with one or more detailed requirements which are expressed as the responsibility of Contractor:

Table 2 – Core M&O Services in Scope

FUNCTIONAL AREAS AND SUB-AREAS
Application Maintenance and Operation Services
• Managed Application Support
• Corrective and Emergency Maintenance
• Preventive Maintenance
• Adaptive Maintenance
• Application Maintenance Tuning
• Application Quality Assurance
• Existing Interface and Existing Integration Support
• Database Administration and Support
• Configuration Management
• Production Schedule Services

• Backup and Recovery Services
• Middleware Support Services
• Performance and Capacity Planning and Management
• Maintenance Services
• Patch Management Services
• Release Services
Availability Management
Capacity Management
DBMS and Clusterware Services
Disaster Recovery
Enterprise Content Management
Escalation Management
Event Management/Monitoring
Identity and Access Management
Knowledge Management
Release Management
Request Services
• Service Desk Services
• Service Desk Support
• IT Service Management (ITSM) Services
• Incident Management Services
• Problem Management Services
• Change Management Services
• Service Requests
Security Services
Service Asset and Configuration Management
Siebel Services
Transition Services

6.1.3 Automated Regression Test Suite M&O: Effective beginning August 15, 2021 Automated Regression Test Suite M&O has been removed from scope.

6.2.1 ITSM

Contractor will provide and manage for utilization by State, Contractor and other service providers, the web-based IT Service Management (ITSM) tool, ServiceNow.

ServiceNow will be the repository for all currently active ITSM tickets as well as all ITSM tickets opened thereafter in ServiceNow and will be established as the standard ITSM system for all HSEP service providers.

Contractor shall formally document and include in the State Security Plan (SSP) deliverable, a complete description of the security framework and controls implemented for ServiceNow. This segregation will allow State, Contractor, and Third-Party Vendors of the State access and will restrict access to certain records, and to certain specific security roles and ITSM functions. The State's users can perform "read-only" functions, including create requests, search the knowledge base, access public pages, initiate chat sessions, view published reports and utilize the service catalog, which are not dependent on ServiceNow Fulfiller licenses (as defined below).

State agrees to use ServiceNow Fulfiller licenses, which are named user licenses that allow for the State to create and modify records, create reports, and perform operational activities. Contractor will provide ServiceNow Fulfiller licenses for up to 30 users to be identified by State's Authorized Representative. Additional Fulfiller licenses may be purchased in blocks of ten (10), as set forth in Attachment B. Contractor will implement the ServiceNow configuration. Contractor agrees that State users will be able to use ServiceNow, with the same data, as Contractor users, while isolating State data in a manner that will adhere to State and federal laws, regulations, rules and policy.

State shall assign a ServiceNow administrator within 60 days of Contract execution or the Effective Date, whichever is later, to support State's administrative requirements, such as authorizing users and access levels for those users to various functions inside of ServiceNow, in the sole discretion of the State.

Contractor agrees that completion of the ITSM transition work will not be considered complete until: a) the ServiceNow implementation is integrated with Contractor's existing CMDB system, and that this integration results in the ability to maintain reportable linkages between tickets and Configuration Items (CIs), and b) historical open ticket data from the existing ITSM system is transferred, or otherwise made available for use within the ServiceNow ITSM system such that the ServiceNow tool and data available therein can be used to improve root cause analysis, and to reduce time required to resolve defects. Historical closed ticket data shall be available to the State in archive status.

6.2.2 Reconciliation Services

Contractor will provide reconciliation services as requested by the State from time to time to correct or align data in the VHC HSEP platform and integrated external systems, including, without limitation, reconciliation services needed to support the State's CMS-mandated monthly enrollment data reconciliation process, which compares certain VHC enrollment data with Qualified Health Plan issuer enrollment data. Generally, Contractor will use reasonable, good-faith efforts to address State's Reconciliation Service Requests (RSRs) without unreasonable delay. With respect only to the specific type of RSR referred to by State and Contractor as an 834 Transaction Removal, Contractor shall prioritize such RSRs between a Priority 2 Incident and a Priority 3 Incident. 834 Transaction Removal RSRs will be addressed with reasonable and good-faith efforts prior to the next scheduled 834 batch transmission provided requests are received from State at least 60 minutes prior to a scheduled 834 batch transmission. RSRs other than 834 Transaction Removal shall be submitted by State through the ITSM system and titled "Recon Service Request" in the Short Description field in the ITSM system. All RSRs shall be submitted by the State through the ITSM system and may only include one Case per RSR.

6.2.3 Application Lifecycle Management (ALM) Software

Contractor shall provide State access to its Third Party Software ALM tool ("ALM Software"). Contractor shall provide State Third Party Vendor(s) access to its ALM Software, if allowed under ALM Software license. This ALM Software shall generally meet the requirements listed in Exhibit 1, Section 18. The Contractor shall maintain the ALM Software and provision access as mutually agreed by Contractor and State. The ALM Software shall be updated according to Contractor best practices. Contractor may change the specific software fulfilling the ALM Software requirements at its sole discretion and shall provide notice to State in advance of any such change. Any change to a different ALM software or other changes to existing ALM functionality requested by State may be subject to additional cost or Change Request.

The ALM Software shall be used in collaboration by Contractor and State for testing and defect management of M&O releases. ALM may also be used for Discretionary Service Request development projects, the scope of such use shall be defined in the associated Change Request.

6.3 Root Cause Analysis - Approach

The Parties agree that the determination of the root cause of P1 and P2 incidents is essential to the attainment of Service Level Agreements (SLAs) and to the efficient administration of the maintenance and operation of all Managed Applications. Therefore, as part of the Problem Management process, which is included in the M&O Manual Deliverable, Contractor and State will define and document a Root Cause Analysis approach for P1 and P2 incidents that is mutually acceptable to the parties. Contractor and State agree to provide the Root Cause Analysis approach document to all HSEP parties and will upload it to a mutually agreed upon location as an HSEP standard. This document will, where possible, establish a sequence of events and target timeline(s) to understand the relationship between contributory, or causal factors, root cause(s), and the defined problem or event, sufficient to guide the development of remediation actions which can prevent a recurrence of the same problem or event in the future.

6.4 HSEP M&O Deliverables and Reports.

6.4.1 The M&O Deliverables are broken into two categories of deliverables:

A) Key Deliverables – Deliverables that require Acceptance by the State and are tied to Deliverable Payment milestones as set forth in Attachment B. Key Deliverables are set forth in Table A below.

B) Non-Key Deliverables – Deliverables that require Acceptance by the State but are not tied to Deliverable Payment milestones. Instead these Deliverables are tied to the Core M&O Services as set forth in Attachment B.

Table A – M&O Deliverables includes the: (1) Deliverable Identifier (“Req”) Number; (2) Key Deliverable Designation (Yes/No); (3) Requirement Name; (4) Deliverable Expectation Document (DED) Submission Timeframe; (5) Deliverable Submission Timeframe; and (6) Update Frequency.

- All DEDs for Deliverables (Key and Non-Key) require Acceptance by the State.
- All updates to Key Deliverables require Acceptance by the State and are tied to payment milestones as set forth in Attachment B.
- All initial updates to Non-Key Deliverables, require Acceptance by the State, and are tied to the Core M&O Services monthly fee.

Table A – M&O Deliverables

Req #	Key Deliverable (Yes/No)	Requirement Name	DED Submission Timeframe	Deliverable Submission Timeframe	Update Frequency
1.K01		RESERVED			
1.K02	Yes	Disaster Recovery Plan	3 Weeks after Effective Date	4 Weeks after DED Approval	Annually
1.K03	Yes	M&O Manual	3 Weeks after Effective Date	4 Weeks after DED Approval	Every Six Months
1.K04		RESERVED			
1.K05	Yes	Architecture Document	6 weeks after Effective Date	4 Weeks after DED Approval	Every Six Months
1.K06	Yes	Availability Plan	6 weeks after Effective Date	4 Weeks after DED Approval	Annually
1.K07	Yes	Configuration Management Plan	9 weeks after Effective Date	4 Weeks after DED Approval	Annually
1.K08	Yes	SSP (State Security Plan)	16 weeks after Effective Date	4 Weeks after DED Approval	Quarterly
2.N01	No	ITSM System	N/A	N/A	N/A
2.N02	No	Knowledge Management Plan	6 weeks after Effective Date	4 Weeks after DED Approval	Every Six Months
2.N03	No	Capacity Plan	9 weeks after Effective Date	4 Weeks after DED Approval	Annually
2.N04	No	Event Management Plan	9 weeks after Effective Date	4 Weeks after DED Approval	Every Six Months
2.N05	No	Source Code Management Plan	16 weeks after Effective Date	5 Weeks after DED Approval	Annually
2.N06	No	System Performance and Reliability Plan	16 weeks after Effective Date	5 Weeks after DED Approval	Every Six Months
2.N07	No	Defect Management Plan	12 weeks after Effective Date	5 Weeks after DED Approval	Every Six Months
2.N08	No	Batch Scheduling Plan	12 weeks after Effective Date	5 Weeks after DED Approval	Quarterly
2.N010	No	Release Management Plan	16 weeks after Effective Date	5 Weeks after DED Approval	Annually

It is understood and agreed that:

- The content of all M&O Deliverables delineated in Table A shall, where applicable, be based upon, and therefore be substantially similar to, the versions of the Deliverables previously delivered to State by Contractor pursuant to the Contract between the State and Contractor dated as of January 1, 2015 (the "Prior M&O Contract").
- All timelines set forth in Table A are dependent on Contractor and State adhering to Attachment A, Section 13: DED Review and Approval Process; and Attachment A, Section 15: Deliverable Review and Approval Process.
- Notwithstanding the DED Submission Timeframe set forth above, in the event the Contactor has already drafted a DED that the State has accepted for a specific Deliverable, Contractor will present the existing DED to State within 2 weeks of Contract Effective Date. Upon the State's Acceptance of the existing DED, the timeframe set forth in the Deliverable Submission Timeframe shall commence.

- If the first submission of a monthly or quarterly Deliverable does not align with the start of a calendar month or quarter, Contractor shall align the subsequent deliveries with the first of the next subsequent calendar month or quarter respectively.

6.4.2 Key Deliverables Descriptions: For each Key Deliverable set forth below, Contractor will produce a DED. The purpose of the DED is to define the Acceptance Criteria for each Deliverable delineated below. Each DED will be agreed upon between State and Contractor.

(1) Disaster Recovery Plan (DRP)
Contractor shall create a DRP that identifies processes and implications for executing the DRP. This will include an annual testing strategy; inclusion of Application M&O support; and methods to return service to Production after testing or a failover event. The DRP will identify and meet both Recovery Point and Recovery Time Objectives required by the State, as defined in the Exhibit 2 Service Levels. The Contractor will be responsible for executing activities in the DRP. This plan shall be consistent with best practices (ITIL, ISO and NIST 800-53 revision 4). The scope of the DRP addresses the production, DR and support Environments. Disaster Recovery for the remaining Environments will be addressed on a best effort basis. Contractor shall be responsible for:

i. Remediation plan, subject to State review and approval;

ii. Documentation of the Test Results -- All testing must be accompanied by a remediation plan developed in consultation with the State and subject to State review and approval. The remediation plan will address failures and plan and timeframes for remediation;

iii. Maintaining and updating the DRP;

iv. Integration of changes introduced to VHC; this includes Change and Configuration Management integration with the Business Change Process (BCP)/DR process, plan, maintenance and testing;

v. Coordinating mutually agreed upon timeframes for execution of DR tabletop testing failover and failback procedures;

vi. Working with State and designated third parties in order to integrate notifications, communication plans and DR plans as necessary for full recovery of VHC in the event of a disaster;

vii. DRP must include Contractor and State governance and communications plans that will be kept up to date;

viii. Up to 10 hours per Contract year of consulting services for no additional charge; and

ix. One failover tabletop exercise for each DR plan annually that tests the Disaster Recovery Technology, Procedures and Communications. As part of the annual Tabletop DR Exercise, Contractor will demonstrate that all Production files are properly replicated to the DR environment. This demonstration will occur using WebEx or other suitable technology to allow State to see that the files replicated from Production are identical in the DR environment.

(2) M&O Manual
Contractor shall develop for the State's review and Acceptance, an M&O Manual that is consistent with existing State processes and best practices (ITIL, ISO 20000, ISO 27000, NIST). Practices and process must be integrated with State's existing and future processes and practices and align with State's HSEP. The M&O Manual shall describe the way Contractor performs its day-to-day activities with the State and the State's Third-Party Vendors. The M&O Manual shall include goals and objectives for each document and the processes, procedures, work flows, RACI matrices, definitions, policies, guidelines, governance model, data and organizational integrations (manual or otherwise), continuous improvement plans and the KPIs, reports and SLAs (as required pursuant to this Contract). The M&O Manual shall include the following processes, functions and activities:

i. Incident, Problem, Service Request Fulfillment, Event and Access Management;
ii. Release Entry Framework;
iii. Change, Release, Asset & Configuration Management;
iv. Contractor's Support Center and Operations Management;
v. Service Level Management; and
vi. Provisioning and de-provisioning users.

(3) Architecture Document
Contractor will maintain an Architecture Document to represent the current configuration standards of the Environment. The Architecture Document will include a topology of how HSEP Managed Applications interact.

(4) Availability Plan
An Availability Plan that contains the following shall be provided by the Contractor and reviewed and approved by State:

i. Availability application architecture for high availability which includes a load balancing strategy;
ii. Availability of Contractor Personnel to meet business requirements for a 24x7x365 service;
iii. Monitoring strategy for providing availability monitoring;
iv. Availability strategy for Managed Applications;
v. Process for proactively creating Incident Tickets (within the agreed Ticketing system), if availability issues are pending or reactively if an availability issue has occurred;
vi. Processes, calculations, and activities for reporting and alerting for failure to meet applicable Service Levels; and

vii. Process for opening RFCs will follow the State's existing Change Management documentation, if monitoring/Incidents require change to Service/CI.

(5) Configuration Management Plan
Contractor shall provide a Configuration Management Plan that will include the following topics and sections:

i. How Contractor will maintain a Configuration Management Database (CMDB) on behalf of the State that contains Configuration Items, attributes, and relationships for the Service being provided. The CMDB shall be managed by a documented configuration management process and under the control of Change Management;
ii. Processes for the identification, control, recording, reporting, auditing, and verifying service assets and configuration items managed on behalf of State. The intention of capturing CIs, attributes and relationships is for impact analysis during changes, troubleshooting for Incidents and Problems, and keeping computing environments in sync;
iii. A policy/plan for working with State and other DDI providers for continuous improvement;
iv. A Responsibility Matrix (RACI) that outlines the roles within the process;
v. Documented plan for keeping computing environments (software and hardware) sufficiently synchronized to confirm testing and release integrity. These include Production, Non-Production, and DR environments;
vi. Staffing required to build, manage, and maintain the CMDB;
vii. Strategy and procedure for tracking and reporting on State owned software assets and licenses for the HSEP M&O Services that are within Contractor's scope of responsibilities; and
viii. Strategy for providing State reporting (and raw data upon request) based upon KPIs, metrics outlined within these NFRs.

(6) SSP (State Security Plan)
Contractor shall, in consultation with the State or its designated Third-Party Contractor, document in the SSP in-scope M&O-related security and privacy control implementation details as set forth in MARS-E Version 2.0 that accurately reflects the Environments where production data reside. The State will review and approve the finalized SSP.

i. State Security Plan Supporting Artifacts **-** Contractor shall maintain an accurate set of compliance artifacts required per Part D of the MARS-E Version 2.0 SSP entitled, "SSP Attachments."

ii. State Security Plan Support - Contractor shall provide written descriptions and/or participate in interviews with the State or the State's designated Third Party for the purpose of accurately documenting the control implementations as required by CMS MARS-E Version 2.0 and IRS Publication 1075. Contractor shall be responsible for providing control implementation descriptions for all controls within CMS MARS-E Version 2.0 and IRS Publication 1075. Control descriptions shall be reviewed and updated by the Contractor at a minimum annually and as needed as a result of any significant change to the environment as defined by CMS.

6.4.3 Reports: These are written reports that require Contractor to use a certain format that are to be submitted in accordance with the Submission Timeframe identified in Table B below, but these reports do not require Acceptance by the State. Reports are tied to Core M&O Services and are found in Table B below.

Table B – Reports includes: (1) the Identifier ("Req") Number; (2) the Report Name; and (3) the Submission Timeframe.

- Reports do not require Acceptance by the State.
- Reports are tied to Core M&O Services monthly fee as specified in Attachment B.

Table B: Reports for Core M&O Services

Req #	Report Name	Submission Timeframe
2.D02	RESERVED	
2.D03	RESERVED	
2.D04	RESERVED	
2.D05	RESERVED	
2.D06	Event Reporting	10th business day of the month, starting the second month of the Contract
2.D07	RESERVED	
2.D08	Managed Application Version Reporting	10th business day of the month, starting the second month of the Contract and quarterly thereafter
2.D09	RESERVED	
2.D10	Release and Change Management Reporting	10th business day of the month, starting the second month of the Contract
2.D11	Service Level Reporting	10th business day of the month, starting the second month of the Contract
2.D12	Status Reports	10th business day of the month, starting the second month of the Contract, and weekly thereafter
2.D13	RESERVED	
2.D19	RESERVED	
2.D20	Roles & Responsibilities Report	10th business day of the month, starting the second month of the Contract and quarterly thereafter
2.D21	Software Configuration Management Report	10th business day of the month, starting January 2019 and quarterly thereafter

Reports delineated in Table B shall, where applicable, be in the format agreed to by and between Contractor and State and as set forth in the M&O HSEP Report Description Document, which may be amended from time to time by mutual agreement of both parties and shall be deemed incorporated herein.

Contractor shall produce and provide to the State the reports set forth above with respect to the Core M&O Services. The Contractor shall add KPIs to these reports as requested by the State and mutually agreed to by Contractor in support of the business and continuous improvement.

6.4.4 Transition Deliverables:
Table C – Transition Deliverables includes: (1) the Deliverable Identifier ("Req") Number; (2) the Requirement Name; and (3) Due Date.

- Transition Deliverables are non-Key Deliverables that do require Acceptance by the State.
- Transition Deliverables are tied to Core M&O services monthly fee as specified in Attachment B.

Table C: Transition Deliverables

Req. #	Requirement Name	Due Date
3.T01	Lessons Learned document	30 days prior to Contract termination
3.T02	M&O Schedule	90 days prior to Contract termination
3.T03	Project Management Plan	90 days prior to Contract termination

(1) Project Management Plan (PMP)
A comprehensive plan for the approach to managing the needs of the business. This shall be agreed upon by Contactor and State. The PMP will include Quality Assurance/Quality Control (QA/QC) and communication processes.

(2) M&O Schedule
An ongoing schedule to be updated and sent to the State Authorized Representative at least monthly, for anticipating and tracking changes to all project tasks, deliverables and milestones. The schedule will sequentially list all tasks to be completed and identify the assigned resources, Start Date, End Date, percent completed, and any dependencies to other tasks.

6.5 License Reporting.
Contractor shall provide the State with the following information regarding the State's Oracle software licenses and other State-paid software licenses installed on the HSEP on a quarterly, or more frequent basis as agreed upon by the parties, as part of Reporting for M&O Services specified in this section:

1. An Inventory of all of State's software licenses installed in all environments managed within the scope of this Contract.
2. The Inventory shall include:
   a. The product name, version, number of licenses and vendor contact information;
   b. A list of installed product components;

c. Oracle Extended Support dates for each component;
d. Specification of the characteristics of the physical and/or virtual server where the licensed software is running, including the number of physical or virtual CPU cores and other server characteristics as available to determine or enable a license count that helps satisfy the State's software license reporting requirements; and
e. List of license keys to be sent to State via mutually agreed secure process.

7. TRANSITION SERVICES

(1) Overview

In addition to the M&O Deliverables set forth in Attachment A, Section 6, Table A above, Contractor shall provide the following Transition Services in the event State should transition to a new vendor for M&O services.

(2) Transition Services

Upon nearing the end of the final term of this Contract, and without respect to either the cause or time of such termination, the Contractor shall take all reasonable and prudent measures to facilitate the transition to a successor provider, to the extent required by the State. The primary activities in this turnover are focused on transition planning to ensure operational readiness for the State and/or successor provider. This includes both a Transition Services period, and the turnover of the Managed Applications and supporting services to the State and/or successor provider. The State shall sign-off on each defined transition milestone to ensure that all transition Deliverables (set forth below), and exit criteria are fully executed based on agreed upon Contract terms. Upon the sooner of a date specified in a notice of termination from either party, and as agreed to by the parties, or within 90 days of Contract expiration, the Contractor shall:

Deliverable 1 - Develop a System Turnover Plan at no additional cost to the State. The Solution Turnover Plan shall include, at minimum:

- Proposed approach to Turnover;
- Tasks and subtasks for Turnover;
- Schedule for Turnover;
- Entrance and exit criteria;
- Readiness walkthrough process;
- Documentation update procedures during Turnover; and
- Description of Contractor coordination activities that will occur during the Turnover Phase that will be implemented to ensure continued functionality of the Managed Applications and services as deemed appropriate by the State.

Deliverable 2 - Develop a Solution Requirements Statement at no additional cost that would be required by the State and/or successor provider to fully take over the Managed Applications, technical, and business functions outlined in the Contract. The Statement shall also include an estimate of the number, type, and salary of personnel required to perform the other functions of the project work and all supporting services. The Statement shall be separated by type of activity of the personnel. The Statement shall include all facilities and any other resources required to operate the Managed Applications, including, but not limited to:

- Telecommunications networks;
- Office space;

- Hardware;
- Software; and
- Other technology.

The Statement shall be based on the Contractor's experience in the operation of the Managed Applications and shall include actual Contractor resources devoted to operations activities.

Deliverable 3 - Develop and submit a Transition Plan including, at minimum:

- Proposed approach to transition;
- Proposed approach for conducting a knowledge transfer from the Contractor to the State or successor provider;
- Proposed approach for consolidating applicable sections from the Contractor's Turnover Plan into the transition planning activity;
- Tasks and activities for transition;
- Personnel and level of effort in hours;
- Completion date;
- Transition Milestones;
- Entrance and exit criteria;
- Schedule for transition;
- Production program and documentation update procedures during transition;
- Readiness walkthrough;
- Parallel test procedures;
- Provider training; and
- Interface testing.

The Contractor shall execute the Transition Plan and activities at no additional cost.

The Contactor agrees, after receipt of a notice of termination, and except as otherwise directed by the State, the Contactor shall:

1. Stop work under the Contract on the date, and to the extent, specified in the notice;
2. Within five (5) business days deliver to the State all State Data and historical project records, including an export of the State Data contained in ALM using the ALM Software supported export functionality, in a form acceptable to the State, and copies of all subcontracts and all third-party contracts executed in connection with the performance of the Services;
3. Place no further orders or subcontracts for Services, except as may be necessary for completion of such portion of the work under the Contract that is not terminated as specified in writing by the State;
4. Assign, to the extent applicable or as the State may require, all subcontracts and all third-party contracts executed in connection with the performance of the Services to the State or a successor provider, as the State may require;
5. Perform, as the State may require, such knowledge transfer and other services as are required to allow the Services to continue without interruption or adverse effect

and to facilitate orderly migration and transfer of the services to the successor provider;

6. Complete performance of such part of the work as shall not have been terminated; and
7. Take such action as may be necessary, or as the State may direct, for the protection and preservation of the property related to this Contract which is in the possession of the Contractor and in which the State has or may acquire an interest and to transfer that property to the State or a successor provider.

Contractor acknowledges that, if it were to breach, or threaten to breach, its obligation to provide the State with the foregoing assistance, the State would be immediately, and irreparably harmed and monetary compensation would not be measurable or adequate. In such circumstances, the State shall be entitled to obtain such injunctive, declaratory or other equitable relief as the State deems necessary to prevent such breach or threatened breach, without the requirement of posting any bond and Contractor waives any right it may have to allege or plead or prove that the State is not entitled to injunctive, declaratory or other equitable relief. If the court should find that Contractor has breached (or attempted or threatened to breach) any such obligations, Contractor agrees that, without any additional findings of irreparable injury or other conditions to injunctive or any equitable relief, Contractor will not oppose the entry of an order compelling its performance and restraining Contractor from any further breaches (or attempted or threatened breaches).

8. PLANNED REPLACEMENTS TO HSEP M&O SERVICES SCOPE

The below identified HSEP Managed Applications are in the process of transitioning to alternate External Systems outside of Contractor's scope of services with the exception of the requirements specified in 8.1.c and 8.2.b below:

- Enterprise Content Management (ECM);
- Business Intelligence (OBIEE).

8.1 Enterprise Content Management. After deployment of the State's Enterprise Content Management (ECM) external system, a Third-Party Software, into the Production environment the State shall submit a written request to the Contractor to shut down the existing ECM Managed Application. Contractor shall shut down the ECM Managed Application within 10 business days of receiving the State's request, unless otherwise mutually agreed by Contractor and State.

A separate request to the Hosting vendor will be required from State to decommission the corresponding servers for the identified Managed Application.

Effective as of the next calendar month after the month in which Contractor shuts down the ECM Managed Application, the Core M&O Services monthly fee shall be reduced by the amount listed in Section 9.1.f. of Attachment B, and the ECM Managed Application's scope shall be deemed modified as follows:

a) "Enterprise Content Management" will no longer be an HSEP Managed Application; and
b) The following requirements will be removed from Exhibit 1:

Functional Area	Sub Area	Req. #	Requirement
Enterprise Content Management Services	General Requirements	**6.000**	Confirm proper operation of the ECM infrastructure.
Enterprise Content Management Services	General Requirements	**6.001**	Support and resolve issues elevated from ADPC, BASU & AHS IT for problems encountered using deployed capabilities of ECM architecture (WC, provisioning, authentication, Fed Cloud access).
Enterprise Content Management Services	General Requirements	**6.002**	Perform schema changes to support application and environment changes.
Enterprise Content Management Services	General Requirements	**6.003**	Participate in maturity of ECM Governance, managed by the State.
Enterprise Content Management Services	General Requirements	**6.004**	Provide maintenance and support for middleware and supporting utilities, perform middleware system recovery, and perform controlled stops and restarts to ECM servers as needed.
Enterprise Content Management Services	General Requirements	**6.005**	Contractor shall perform those services, functions and responsibilities identified as their respective responsibilities with respect to the installation, configuration, and management of the Enterprise Content Management (ECM).
Enterprise Content Management Services	General Requirements	**6.006**	The Contractor shall participate in governance and change management process.
Enterprise Content Management Services	General Requirements	**6.007**	Provide, install, configure, maintain, and monitor availability, reliability, and performance of ECM for OEM (WebCenter (WC) Suite, WC Capture, WC Recognition, WC Content, WC Capture Server, WC Recognition Server, WebCenter Content Server, Web Logic Server, SFTP Server, Database, SOA Connection and WebUI at Contractor recommended patch levels to meet business performance requirements.
Enterprise Content Management Services	General Requirements	**6.008**	Maintain and operate the five instance configurations (Development, Test, Training, Stage, and Production), for ECM, including the maintenance and operation of a mechanism by which external partners can send content into the ECM.

Enterprise Content Management Services	General Requirements	**6.009**	ECM Monitoring: • Manage and monitor SLAs including availability, reliability, throughput, and capacity. • Perform logging and Monitoring of ECM Infrastructure. • Maintain the service composites. • Perform runtime Service Usage Tracking, Monitoring, Alert Notifications, and Exception Management. • Maintain Federal Cloud connectivity.
Enterprise Content Management Services	General Requirements	**6.010**	Error Logs for WC maintained and reviewed and reviewed on a daily recurring frequency.
Enterprise Content Management Services	General Requirements	**6.011**	Run and maintain the daily scripts to produce daily WC reporting.
Enterprise Content Management Services	General Requirements	**6.012**	Maintain ECM error log, perform reviews of logs and manage error log email-distribution list.
Enterprise Content Management Services	General Requirements	**6.013**	Perform failover and failback operations as part of scheduled and unscheduled DR events.
Enterprise Content Management Services	General Requirements	**6.014**	The Contractor shall support the troubleshooting, monitoring and usage of the ECM infrastructure.

c) The following requirements will be added to Exhibit 1:

Functional Area	Sub Area	Req. #	Requirement
Enterprise Content Management Services	General Requirements	**6.000**	Contractor shall perform those services, functions and responsibilities identified with respect to the installation, configuration and management of the ECM interfaces including infrastructure components, which will enable the exchange of data both within the internal systems and with State Private Cloud reporting instances.
Enterprise Content Management Services	General Requirements	**6.001**	Confirm transmission and receipt of webservice transactions through VHC integration with ECM.
Enterprise Content Management Services	General Requirements	**6.002**	Triage issues elevated from ADPC, BASU & ADS AHS IT for problems encountered using system capabilities of ECM architecture (authentication, webservices, interconnectivity).

Enterprise Content Management Services	General Requirements	**6.003**	The Contractor shall participate in any required governance and change management process as needed including interface or environment changes.
Enterprise Content Management Services	General Requirements	**6.004**	Maintain and operate the Production and Non-production environments for ECM, including the maintenance and operation of ECM interfaces and transmissions with external partners.
Enterprise Content Management Services	General Requirements	**6.005**	Maintain middleware error log, perform reviews of logs, and manage error log email-distribution list.
Enterprise Content Management Services	General Requirements	**6.006**	Participate in failover and failback operations as part of scheduled and unscheduled DR events.

8.2 Business Intelligence (OBIEE)
After deployment of the State's business intelligence reporting external system, a Third-Party Software, into the Production environment, the State shall submit a written request to the Contractor to shut down the existing OBIEE Managed Application. Contractor shall shut down the OBIEE Managed Application within 10 business days of receiving the State's request, unless otherwise mutually agreed by Contractor and State.

A separate request to the Hosting vendor will be required from State to decommission the corresponding servers for the identified Managed Application.

Effective as of the next calendar month after the month in which Contractor shuts down the OBIEE Managed Application, the Core M&O Services monthly fee shall be reduced by the amount listed in Section 9.1.f. of Attachment B, and the OBIEE Managed Application's scope shall be deemed modified as follows:

a) "Business Intelligence (OBIEE)" will no longer be an HSEP Managed Application; and
b) The following requirements will be added to Exhibit 1:

Functional Area	Sub Area	Req. #	Requirement
SQL Server Integration Reporting	General Requirements	**11.000**	Contractor shall perform those services, functions and responsibilities identified with respect to the installation, configuration and management of the Active Dataguard replication process including infrastructure components and their related interfaces which will enable the exchange of data both within the internal systems and with State Private Cloud reporting instances.
SQL Server Integration Reporting	General Requirements	**11.001**	Manage and monitor availability, reliability, and performance of Active Dataguard replication components to meet the expectations of the solution.

SQL Server Integration Reporting	General Requirements	**11.002**	Perform full or partial database re-instantiation and reconfiguration of Active Dataguard, as needed, in the event of replication sync failure.
SQL Server Integration Reporting	General Requirements	**11.003**	The Contractor shall participate in any required governance and change management process as needed.
SQL Server Integration Reporting	General Requirements	**11.004**	Maintain and operate the three instance configurations (DEV3, Stage, and Production), for Active Dataguard, including the maintenance and operation of a mechanism by which data can be replicated to corresponding State instances.
SQL Server Integration Reporting	General Requirements	**11.005**	The Contractor shall support the troubleshooting, monitoring, usage, and triage of Active Dataguard including replication logs.
SQL Server Integration Reporting	General Requirements	**11.006**	Confirm and validate proper transmission, receipt, and operation of data population into VHC from external reporting system(s)

9. OUT OF SCOPE HSEP M&O SERVICES

The following functions and responsibilities are specifically outside the Contractor's scope of services under this Contract:

(1) HSEP M&O Services for any systems and applications that are not listed above in Attachment A, Section 6.1, Table 1 and Table 2; which as of the Effective date of Amendment #2, Master Data Management has been removed from Contractor's scope of services;

(2) HSEP Managed Applications security testing, vulnerability scanning, and penetration testing and other security risk assessments, and preparation of the Privacy Impact Assessment (PIA) documentation;

(3) All functions and responsibilities related to the HSEP M&O Services that are not expressly identified in this Contract as within Contractor's scope of responsibility under this Contract;

(4) Consulting services, except as set forth in in Exhibit 2, specifically for the Disaster Recovery Plan;

(5) Hosting Services;

(6) Business operations and process outsourcing services;

(7) The sufficiency, scope and delivery of testing and quality management services for the HSEP Managed Applications under the State's Contract for design, development and implementation services ("DDI"). Contractor's sole responsibility under this Contract in connection with such activities shall be to provide limited advice to the State at the State's direction under this Contract;

(8) Third party software, systems and data interfaces ("External System") are not the responsibility of Contractor, other than those provided or supported by Contractor hereunder or under another agreement with the State. To the extent that any changes to an External System would require a change to the Managed Applications, such change will need to be completed pursuant to a Change Order agreed to by the Parties. For clarity, the foregoing does not relieve Contractor of its responsibility to manage any Incident with respect to the Managed Applications that result from any change made to an External System; provided however, where Contactor has not been provided with advance notice of such the Change to the External System and has not agreed to a change pursuant to an agreed Change Order, the resolution of such Incident may require that the change to the External System be backed out (e.g., the External System will need to be reverted back to the pre-change state);

(9) Integration failures of the State and State Third Party Vendor(s) (excluding Contractor under this or any other agreement); and

(10) The issuance of any Major Release(s), provided that Contractor shall oversee the release management for the State's DDI Vendor.

10. MANAGEMENT TEAM

Contractor shall provide a Management Team comprised of the following Key Staff roles that may be held by one or more people. Roles and responsibilities may be modified at Contractor's discretion to enable Contractor to provide the HSEP M&O Services to the State in accordance with this Contract. Contractor shall provide an organizational chart to the State upon written request. Contractor shall promptly notify the State of any changes to Management Team and Key Staff. Contractor shall provide a Management Team comprised of Key Staff as follows:

(1) Key Staff Management Team Roles:

a. Engagement Lead (also referred to herein as the Project Manager);
   i. Contractor will provide a Project Manager ("PM") and his/her effort will incorporate the tasks necessary to implement all activities and to provide all HSEP M&O Services as specified in this Contract; and
   ii. Contractor's PM or designee shall participate in all governance meetings as mutually agreed.

b. Operational Manager;
   i. Contractor's Operational Manager and his/her effort will incorporate tasks necessary to comply with this Contract.

c. Service Delivery Manager
   i. Contractor's Service Delivery Manager will lead the break/fix activities, including the prioritization of work and coordination with Third Party Vendors of the State.

d. Service Coordinator

i. Contractor's Service Coordinator will lead the triage and ticketing processes, serving as an escalation point for unresolved P1 and P2 issues; and

ii. Contractor's Service Coordinator will be the State's primary contact for the ITSM solution, "ServiceNow."

e. Release Manager shall be responsible to:

1. Oversee the promotion of code through the State's environments;
2. Provide release-related information to the State for its review; and
3. Represent M&O criteria and its impact on the HSEP platform on behalf of State at the OCRB.

11. GOVERNANCE ACTIVITIES

The Parties agree that State and Contractor management teams will utilize a governance model that implements oversight and review with a specified frequency, participants and subject matter. To that end, the Parties agree to adopt a model which includes the following elements:

(1) **Weekly Review:** Contractor's Operational Manager will review with State's Authorized Representative or his/her designee, on a weekly basis (unless otherwise mutually agreed), daily dashboards, address exceptions and operational issues related to both State and Third-Party Vendors of the State.

(2) **Monthly Review:** Contractor's Operational Manager will, on a recurring monthly basis (unless otherwise mutually agreed), together with State's Authorized Representative or his/her designee, and State's Contract Manager, review: (1) Contractor's Service Level Agreement compliance; (2) perform capacity planning; and (3) recommend process improvement initiatives which shall be noted in the meeting minutes.

Contractor will, on a recurring schedule, together with State's Authorized Representative or his/her designee, and State's Contract Manager, review service delivery quality, State and Contractor resourcing, escalations made since the prior weekly meeting, risks and issues identified since the prior meeting, and any which continue to be open more than one week.

Contractor will, on a recurring schedule, meet with State's Project Manager to monitor during the ITSM transition period, all transition-related risks and issues.

(3) **Quarterly Review:** Contractor's Executive Leadership will meet with State's Executive Leadership on a quarterly basis, unless otherwise mutually agreed, to review overall contractual compliance and to create, review, or revise strategic plans or topics.

12. EXISTING DELIVERABLES/DED CATALOG REVIEW

Within 30 calendar days of the Effective Date, Contractor will provide to State, an evaluation of the existing catalog of Deliverables for the VHC project and will provide a recommendation on a per document basis for the reuse or repurpose of Deliverable templates and DEDs wherever possible for use with the HSEP. Contractor will update the DEDs as set forth in Attachment A, Section 13 below, and Deliverable templates to accommodate the scope of work specified in this Contract and will submit them for State review and approval in accordance with the agreed-upon Deliverable management process as set forth in the PMP within 60 calendar days of the Effective Date. State will then have to respond as set forth in Attachment A, Section 13.

13. DED REVIEW AND APPROVAL PROCESS

(1) Contractor will work with State to develop DEDs and then submit to the State for review.

(2) The State will have five (5) business days to review and approve the DED, or to provide comments if the DED is not acceptable. During this five (5) business day period, the State may schedule and conduct a joint walkthrough of the DED with Contractor so that Contractor can make real-time updates based on State feedback. At the conclusion of the walkthrough, the goal is to confirm that updates to the DED are agreed.

(3) If State provides comments to Contractor on or before the end of the five (5) business day period, Contractor will have three (3) business days to incorporate comments and resubmit the DED to State for electronic approval.

(4) If at the end of this five (5) business day period, the State has neither accepted, nor provided comments on the DED, the DED may be escalated pursuant to Section 18 in this Attachment A.

14. DED REVISION PROCESS

(1) A DED may be reopened for modification (Revised DED) upon mutual agreement of Authorized State Representative and Contractor Operational Manager to address minor changes such as correcting and/or clarifying criteria. It is understood that generally a DED may not be modified more than once per Contract year. Modifications to a DED will be made according to the terms in this section and will be tracked via the Change Request log. Until a Revised DED has been approved by the State, existing DED criteria shall continue to apply.

(2) The State will have two (2) business days upon receipt of Revised DED to confirm that comments provided have been addressed and approve or disapprove the Revised DED. If the State fails to provide approval of the Revised DED, the Contractor and State shall endeavor to resolve any remaining issues within one (1) business day.

15. DELIVERABLE REVIEW AND APPROVAL PROCESS

1. Contractor will submit Deliverable to the State for review.
2. The State will have five (5) business days to review and approve the Deliverable, or to provide comments if the Deliverable is not acceptable.
3. During this five (5) business day period, the State may schedule and conduct a joint walkthrough of the Deliverable with Contractor so that Contractor can make real-time updates based on State feedback. At the conclusion of the walkthrough, the goal is to confirm that updates to the Deliverable are agreed.
4. If State provides comments to Contractor on or before the end of the five (5) business day period, Contractor will have three (3) business days to incorporate comments and resubmit the Deliverable to State for electronic approval. Any comments after this point in the review

process that are not directly related to either the original comments provided in step 2 above, or their updates as provided by Contractor in step 4, will be addressed in the next scheduled delivery of that Deliverable.

5. If at the end of this five (5) business day period, the State has neither accepted, nor provided comments on the Deliverable, the Deliverable may be escalated pursuant to Section 18 in Attachment A.
6. The State will have two (2) business days to confirm that comments provided have been addressed and approve or disapprove the Deliverable. If the State fails to provide approval of the Deliverable, the Contractor and State shall endeavor to resolve any remaining issues within one (1) business day.

16. CONTRACT/PROJECT CHANGE ORDERS

Consistent with Section 6 on page 1 of this Contract, no changes, modifications, or amendments in the term, maximum amount or terms and conditions of this Contract and no material modifications to the Contract scope shall be effective unless reduced to writing, numbered and signed by the Commissioner or Deputy Commissioner of the State and a duly authorized representative of the Contractor.

When estimates are required for changes that may require additional costs exceeding the Maximum Amount, Contractor will provide those estimates at no cost to the State, understanding that any change that requires additional cost shall be reduced to writing and signed by the duly authorized representative of the State and Contractor.

Contractor agrees to negotiate reduction in the costs specified in Attachment B of this Contract, in the event that a Change Order identifies a change which, if implemented, will significantly reduce the level of resources Contractor is required to utilize in order to attain the SLAs stated in this Contract.

17. OPERATIONAL CHANGE REQUEST PROCESS

17.1 General. Contractor and State will follow the change control process identified in the approved Project Management Plan (PMP) and Change Management Plan, which will be delivered per the schedule presented in the Deliverables tables in Section 6 of this Attachment A. Contractor will employ formal change control for the project and will continue to align its Change Management Plan to the State's change management process. For all Change Requests (CRs) entered into the Change Request system to the extent the CR impacts Contractor's responsibilities, Contractor will provide a work estimate to State, together with other descriptive information necessary for State to make decisions. All Discretionary Service Requests (as defined below) shall be developed, processed and approved as CRs, it being understood that Discretionary Service Requests, for which a portion of the Maximum Amount has been reserved, do not require an amendment to the Contract. Discretionary Service Requests shall be construed as "Specification Orders" in the terminology of the State's change management process (the "DVHA Portfolio Change Control Plan").

17.2 IE&E. In the sole discretion of the State, for any Discretionary Service Request supporting the State's Integrated Eligibility and Enrollment (IE&E) Program, the CR describing the work shall require agile project management work practices, and code delivery and acceptance pursuant to a

Quality Assurance Surveillance Plan (QASP) conforming substantially to the State's standard form of QASP included as Exhibit 5 to this Attachment A, with such modifications as may be agreed to be necessary or appropriate for the services specified. The QASP for each Discretionary Service Request under this section shall be attached to the CR specifying the work, and shall, for that work only, take precedence over any other inconsistent or contrary provisions in this Contract.

18. INFORMAL DISPUTE RESOLUTION PROCESS

The parties desire that all disputes arising under this Contract be resolved expeditiously, amicably, and among the day-to-day project managers. The parties shall use good faith to resolve any disputed matter. In the event a material dispute remains unresolved among the project managers after a fourteen (14) calendar day period, the dispute shall be elevated to the Program Director for Contractor and the Deputy Commissioner for a State for a five (5) business day resolution period. In the event a material dispute remains unresolved after five (5) business days, the dispute may be elevated to the Vice President, IT for Contractor and the Secretary of AHS for the State.

Notwithstanding the foregoing, neither party waives any rights or remedies it may have in equity or at law. In the event that a party breaches this Contract, including the right to seek emergency injunctive relief during or prior to the invocation of the Dispute Resolution Processes if required to protect a party's interest.

19. STATE RESPONSIBILITIES

Without limiting its other obligations under this Contract, State shall:

(1) Designate to Contractor, in writing, current emergency contacts, including name, address, telephone, mobile phone and e-mail address. Emergency contacts shall be the primary contacts notified in case of any HSEP M&O Services-related Severity Level 1 or Severity Level 2 incidents and must have ability to make decisions on behalf of the State.
(2) Obtain all licenses necessary for Applications and other intellectual property other than those for which Contractor is responsible. State shall acquire and maintain, during the term of this Contract, all necessary maintenance and support for such Applications and intellectual property.
(3) Provide notice, via email communication, to Contractor's Project Manager, of any business changes at least 48 hours prior to the change that may have an impact on delivery of HSEP M&O Services (e.g., large changes in the expected volume of Users for a Managed Application, modifications in lines of business, or significant changes in the use of a particular Managed Application).
(4) Except as expressly stated otherwise in this Contract, be responsible for all costs and expenses related to remotely accessing and using the HSEP Managed Applications and M&O Services, including acquiring and maintaining the applicable Software, Equipment, and telecommunications services.
(5) Except as expressly stated otherwise in this Contract, configure and manage the Equipment and Software located at State's Facilities, including telecommunications up to the Contractor demarcation point.
(6) Except as expressly stated otherwise in this Contract, be solely responsible for any code, Software, Equipment or services utilized or provided by State, except to the extent provided by Contractor or its subcontractors.

(7) Be responsible for State's use of and access to the Managed Applications and State Data. This includes not using or permitting the use of the Managed Applications in a way that knowingly violates any applicable law. Contractor may disable the access of an individual User who Contractor reasonably believes may be the source of a Security Breach or otherwise threaten the security or integrity of a Managed Application. Contractor shall notify the State in writing if it disables the access of an individual User.

(8) Provide direction to State Third Party Vendors to facilitate Contractor's fulfillment of responsibilities under this Contract.

(9) Be responsible for any core business functions, call center services and business operations not within Contractor's scope of services.

(10) State shall cause its DDI Vendor be responsible for issuance Major Releases.

(11) State shall ensure that prior to effective date of the amendment that the HP UFT is current with version 12.54.

20. STATE DELAYS

Whereas the State is committed to the Maintenance and Operation of the Human Service Enterprise Platform as described in this contract's Subject Matter, the State shall use reasonable efforts to provide staff, resources, and decisions necessary to satisfy its obligations to scope of work defined within this Contract. State shall perform reviews and approvals in accordance with this Contract and other processes agreed by the parties, however the failure to do so in a timely manner shall be deemed to be a "State Delay." The State shall not be deemed in default for any State Delays or other delays in the provision of staff, resources, or decisions as they impact this Contract.

21. DEFINED TERMS

As used in this Contract, the following terms shall have the meanings set forth below.

24 x 7 means 24 hours per day, 7 days per week, and 52 weeks per year.

Acceptance means State agrees the Contractor has met the relevant criteria for the submission.

Access Integration means the State's legacy Integrated Eligibility System.

ADPC means application and document processing center.

ADTM means adjusted downtime minutes.

Application means a Software product on the HSEP.

Available means, with respect to Managed Application, accessible to Users.

Availability means the state of being Available.

BASU means the State's Business Application Support Unit.

Business Day means Monday through Friday, exclusive of locally observed Vermont holidays.

Call Center means the call center operated by State to take calls from Users with respect to the Managed Applications.

Case means all of the current and historical eligibility and enrollment information for a single eligibility application.

CCB (Change Control Board) means the team that oversees approves, and tracks proposed Change Requests. Its members include key members from State and Contractor project, operations and IT teams. The CCB reviews impact with appropriate resources (i.e. Business, Legal, Technical, and Security). It approves and/or rejects Change Requests, prioritizes work effort and sizing and formal level of effort and pricing from Contractor.

Change Control means the process State and Contractor follow to propose and approve a Change Request.

Change means any deliberate action by Contractor that alters the form, fit or function of configuration items (components within a Managed Application) in production that is within Contractor's Scope of responsibility (as set forth in Section 6 of this Attachment A) and under Contractor's control.

Change Order means a component of the Change Management Process, as defined in the Project Management Office Plan, whereby changes in the Scope of Work agreed to by the State and contractor are implemented.

Change Request means a request by Contractor or State via the Change Management process, for a Change to HSEP in production.

Change Window means a period of time in which a Change shall be executed and during which the performance or functionality of the Managed Applications may be unavailable, limited, impaired or degraded.

CI means configuration item, in reference to the unit of configurability for artifacts tracked in the Configuration Management Database (CMDB).

Clusterware means portable cluster software that allows clustering of independent servers so that they cooperate as a single system.

Contractor Personnel means and refers to Contractor's employees and employees of Contractor's permitted subcontractors or permitted agents assigned by Contractor to perform Services under this Contract. To allow Contractor to be able to manage its performance of Services most effectively, Contractor reserves the right to determine which of its qualified Personnel will be assigned to perform Services and to replace or reassign Contractor Personnel during the Contract Term.

DBMS means database management services.

DDI Activities means those activities performed by Contractor under a CR, DDI vendor or other third-party vendor personnel that may be designated as Design, Development, and Integration related activities.

DED means Deliverable Expectation Document.

Disaster means any Unplanned Outage that causes a complete loss of access to and use of the Production Environment for a period greater than 24 hours. Such an outage may occur due to a wide range of events, incidents, or problems that may affect the State, Contractor, Hosting Provider, or other Third-Party Vendors.

Discretionary Service Request (DSR) means those changes that are performed by Contractor at the State's election from time to time, the specific requirements of which shall be determined and documented through the Change Request process provided in Section 17 of this Attachment A. Discretionary Services are not required in order to maintain normal operations and will be paid out of a separate reserved portion of the Maximum Amount specifically allocated to pay for Discretionary Service Requests, up to the amount specified in Attachment B.

Enhancement means any product change or upgrade that increases software functional capabilities beyond original delivered specifications and performed through a Change Request or Discretionary Service Request.

Enterprise Installation Matrix: A document created by Contractor which tracks the current patch levels installed across the HSE and VHC environments.

Equipment means, for this Contract, hardware used in providing the HSEP M&O Services.

Emergency Change means a Change that must be introduced as soon as possible to resolve an open high-severity Incident. It is also known as Incident Change in the Contractor's ticketing system. These are the only Changes that can be documented after the fact.

Forward Schedule of Change (FSC): A document that lists all authorized changes and their planned implementation dates, as well as the estimated dates of longer-term changes. A change schedule is sometimes called a forward schedule of change, even though it also contains information about changes that have already been implemented.

Fulfiller licenses means a type of software license applicable to the ServiceNow ITSM solution, which is a per-user license that provides for user access to ServiceNow functionality based on roles which are defined and configured according to user-organization specification. This is differentiated from Requester, and Approver license types.

FTI means Federal Tax Information.

HSEP means Health Services Enterprise Platform.

HSEP Fees means the Fees identified in Attachment B, Payment Provisions.

HSEP/VHC Business Hours of Operations means M-F 7:45 am - 8:00 pm, Sat 8:00 am – 1:00 pm Eastern Time.

IAM means Identity Access Management.

Incident means an unplanned interruption to an IT Service or reduction in the quality of an IT service. Failure of an item that has not yet affected service may also be an incident – for example, failure of a scheduled database backup.

Incident Management means Contractor's process for monitoring, entering, reviewing and resolving Incident tickets and Service Requests. The objective of Incident Management is to restore functionality of the applicable Managed Application.

ITSM – Information Technology Service Management

JCA means Java Connector Architecture.

JDBC means Java Database Connectivity.

JVM means Java Virtual Machine.

KPI means key performance indicator.

Leaked Defect means a defect that is identified prior to or during UAT but is intentionally deployed into production; typically to allow more critical code to be deployed promptly. The effect(s) of a leaked defect in production and creation of any workarounds are the State's responsibility.

Level 1 Support means the support service that is provided as the entry point for Incidents or inquiries from members. Level 1 Support for Members shall be provided through State's Call Center Services. This level of support is provided by a focused set of skilled, but generalized, agents. If the Level 1 Support personnel cannot resolve the Incident, the Incident is transferred (through a warm transfer where possible) to the appropriate resolver group for resolution, which may include Level 2 Support personnel or a third party.

Level 2 Support means the handling of Incidents or inquiries through a service ticket or transferred contact, troubleshooting the reported situation and providing solutions to resolve the Incident or satisfy the inquiry in the form of recommendations, workarounds, and administrative fixes or referring the Incident to Level 3 Support for resolution. This level of support is provided by a specialized, cross-environment team of highly skilled agents focused on resolving more complex issues, who are managed as a referral point based on clear scripting and direction.

Level 3 Support means the support service provided by the personnel or third party that is most knowledgeable about the underlying Incident (provided by any combination of application operations and maintenance support, engineering and system administration personnel) and that is utilized when efforts to resolve the issue with Level 1 Support and Level 2 Support have failed or have been bypassed. Incidents and Problems requiring Level 3 Support typically require some sort of hands-on activity.

Maintenance Windows means Sanctioned periods of downtime established, set, and approved through the OCRB process, during which Contractor may perform general maintenance functions and during which the performance or functionality of the Managed Applications may be unavailable, limited, impaired or degraded.

Major Release has the meaning of a release of a piece of software, developed by the DDI vendor or another third-party vendor, which is not merely a revision or a bug fix but contains functional feature enhancement changes, with respect to the HSEP Applications. It follows the full SDLC requirements and generally involves more than 250 hours to develop and test. It is understood and agreed that Contractor's scope of services under this Contract do not include the issuance of any Major Release(s) but rather only having Contractor oversee the release management for the State's DDI Vendor.

Managed Application means an Application which is a business component of the HSEP that Contractor supports pursuant to this Contract, the list being set forth in Attachment A, Section 6.1, Table 1 of this Contract. These Managed Applications may be classified as either Software, systems, or business components.

MDM means master data management, which as of the Effective Date of Amendment #2, is no longer included in Contractor's scope of services.

Member means either (1) an insured individual whose enrollment transaction was processed through the applicable HSEP (each such Member will remain a Member as long as the Member remains enrolled in the plan) or (2) an individual whose Medicaid eligibility check was processed by the applicable HSEP, who was redirected to Medicaid enrollment system and who enrolls in a Medicaid plan.

Minor Release has the meaning of a release of a product that does not add new features or content, is intended to solve minor problems such as bugs or security fixes or Non-Discretionary Service Requests, with respect to the Managed Applications, does not require full SDLC, and involves less than 250 hours to develop and test.

Non-Discretionary Service Request (NDSR) means a request documented in the Ticket Management System for a minor change to a Managed Application or for a task, which is not tied to an Incident that is determined by Contractor to be necessary to keep the Managed Application available and functioning in accordance with its applicable Requirements. NDSRs are by definition herein minor enough that they generally do not require the full System Development Lifecycle of Design/Development/Test/Production and generally involve less than 250 hours of development and testing. DDI Activities and Enhancements will not be subject to classification as NDSR. Examples of Non-Discretionary Service Requests include (but are not limited to): Reconciliation Service Requests, data corrections, reference table updates and mapping changes, researching denials, missing information, access requests, Request For Information, Business Rule Updates, Provisioning requests, Process documentation review, Access requests, Requests for raw data, Infrastructure requests, plan code errors, routine archiving and purging of data, recovering lost data from a backup tape, manually restaging files that have been internally corrected or externally updated by State, and other activities required to maintain existing system functionality. Any NDSR must be identified as such in the Ticket Management System, and such designation must be approved by State before any related work commences. Enhancements will not be completed through an NDSR and will only be performed through a Change Request or Discretionary Service Request. Requests that involve development and testing by Contractor above 250 hours may be performed through a Change Request or Discretionary Service Request, unless otherwise agreed to by the parties.

Non-Production means the Development, Testing, Stage, and Training environments.

Notification Event means a security breach of any of the Contractor's security obligations or other event requiring notification hereunder or under applicable law.

OAAM means Oracle Adaptive Access Manager.

OAM means Oracle Access Manager.

OCRB (Operational Change Review Board) is the group of State and Contractor staff that conduct final State review before the change is deployed into the production environment. This step ensures the State is satisfied with test results, technical Impact, back out plans and communicating end user impact & training needed.

OEM means Oracle Enterprise Manager.

OIM means Oracle Identity Manager.

OPA means Oracle Policy Automation in this Contract and does not refer to Open Platform Architecture.

OUD means Oracle Unified Directory.

OVD means Oracle Virtual Directory.

Party or **Parties s**hall mean Contractor and State.

Post-Production Defect means a defect that is only identified once code has been deployed in Production (unlike a Leaked Defect). Post-Production Defects are the responsibility of the DDI vendor that triggered the defect, including the efforts necessary to create a workaround until the defect is fixed.

Primary Business Components means the following subset of the Managed Applications: (1) VHC External Portal, (2) VHC Internal Portal and (3) Siebel.

Priority Level 1 means an Incident that severely impacts or has the potential to severely impact mission critical business operations or has high visibility to external customers. Incidents at Priority Level 1 are characterized by the following attributes:

(a) Loss of a business-critical CI such as a Managed Application, Service, Software, Equipment, network component or facility making the CI:

- Not Available;
- Substantially Unavailable; or
- Seriously impacting to normal business operations.

(b) Affects a group or groups of people performing a critical business function.

Ex: Connectivity to the VHC is down, Inability to Login to the VHC or Siebel, Confirmed Security breach impacting FTI/PHI/PII data, Day 0 virus/worm that may affect the VHC systems, Critical supporting services are unavailable or not accessible to State operations (like Siebel, IDM, WebCenter, ACCESS, OPA), reporting and auditing.

Priority Level 2 means an Incident that significantly impacts mission critical business operations or has moderate visibility to external customers. These incidents are characterized by the following attributes:

(a) Does not render a CI such as a Managed Application, Service, Software, Equipment, network component or facility unavailable or substantially unavailable, but a function or functions are:

- Not Available
- Substantially unavailable or not functioning as they should, in each case prohibiting the execution of productive work

(b) Affects one or more groups of people performing a critical business function.

Ex: Unable to access payment pages, Unable to access multiple cases in Siebel, Federal Hub/Remote ID Proofing down, unable to access OBIEE, Delayed notices impacting Legal deadlines, Incidents having Labor intensive workarounds and inefficient for State, Unable to support Appeal issue with multiple customers due to system issues, Duplicate Payment or invoice processing

Priority Level 3 means an Incident that impacts a non-critical Managed Application or component for a limited number of Users, that impacts the ability of one or a limited number of Users to perform their primary function or is a time critical NDSR. Ex: Missing Payments in Payment history screen but available in the attachment, Verbiage change to portal due to Legislative/Legal compliance/deadlines, or Provisioning Issue related to multiple requests

Priority Level 4 means an Incident that impacts a single User's ability to perform his or her job function. Ex: Issues related single user/family, report discrepancies, single user provisioning issue, and verbiage changes to the portal.

Priority Level 5 means a request that may or may not be related to an Incident. (Used for Service Requests, Request for Information, and Service Complaints). Ex: Ad hoc report generation request, User provisioning request, Assistance in validating the User access or User information (not related to an issue or incident).

Problem means identifying the underlying root cause, as determined by Contractor, of one or more Incidents or known defects introduced into the production environment by a release which may potentially cause an Incident.

Problem Management means Contractor's process of managing the lifecycle of all Problems to prevent Problems, to eliminate recurring incidents, and to minimize the impact of incidents that cannot be prevented. Includes identifying the root cause (when possible) of Incidents and resolving such underlying root cause within the Contractor's responsibilities, with a fix or workaround that is designed in a manner to prevent the Incidents from recurring.

Production means the Production environment, Disaster Recovery, and Support Environments.

Recovery Point Objective or **RPO** means the prior point in time to which State Data shall be restored in accordance with the Disaster Recovery Plan.

Recovery Time Objective or **RTO** means the target amount of time to restore the Managed Applications after a Disaster has been declared.

Release means one or more changes to an Application that contains new error corrections, fixes, patches, and/or new features or functions and that Contractor makes generally available to State.

Restoration means fixing a Priority 1 or Priority 2 Incident or Problem to restore the Managed Application to normal operation. Restoration may be achieved by a temporary workaround.

Root Cause Analysis has the meaning of the process of investigation and diagnosis that leads to the full understanding of the underlying cause.

Root Cause Debrief is the preliminary information available regarding a Problem, including symptoms, potential causes, next steps and lesson(s) learned during incident restoration.

Service Attribute means a placeholder for information that applies to a specific service only. The actual values of these fields are provided a service is delivered or returned.

Security Incident means a violation or imminent threat of violation, as defined in NIST Special Publication 800-61 Revision 2, to computer security policies, acceptable use policies, or standard security practices that affect any Managed Application. For this Contract, applicable security policies are as defined in Attachment A, Exhibit 1.

Service Desk means the service desk provided by the State.

Service Desk Services means support that the Contractor provides to the Service Desk.

Service Request means either an NDSR or DSR from the State in ITSM for a task, which is not tied to an Incident, to be considered by the Contractor to fall within the Contractor's scope of responsibilities under this Contract.

SFTP means Secure File Transfer Protocol.

SOA means Service Oriented Architecture.

Software has the meaning of instructions executed by a computer, including, at minimum, executable machine code.

Splunk is a tool used to monitor and analyze systems.

Standard Change means a Change that is repeatable, low risk, and relatively common, and for which procedures are in place to follow a pre-defined, relatively risk-free path, and is the accepted response to a specific requirement or set of circumstances, where Change authority's approval is effectively given in advance of implementation. It is also known as Pre-approved change in the Contractor's ticketing system.

State shall mean State of Vermont, Agency of Human Services, Department of Vermont Health Access, or Agency of Digital Services personnel.

State Representative means a designated representative of State that is authorized, by Document of State and Contractor, to contact the Service Desk, access the Ticket Management System, and submit information regarding Incidents and Service Requests.

Support Environment means software components used to support and monitor the Production environments.

Third Party Contractor means Third Party Vendor.

Third Party Software has the meaning of any software from a Third-Party Software Vendor, which is not provided by Contractor as part of the HSEP, and any software developed or provided by State.

Third Party Vendor means a provider procured by the State, other than Contractor, of products or services that are not within the Contractor's Scope of Work for the Managed Applications under this Contract. For purposes of clarity, if and to the extent Contractor for the products and services in this Contract is also the Contractor for hosting services under a separate hosting contract with the State, such hosting services contractor shall still be considered a Third Party for purposes of this Contract.

Ticket means the documentation or electronic record for an Incident, Problem or Service Request, which is opened to identify the existence of a Service Request and remains open until the Incident, Problem or Service Request has been Resolved.

Tools mean testing, monitoring or other tools or utilities and related know-how, methodologies, processes, technologies, or algorithms.

Urgent Service Change means a change which cannot wait the necessary time required for approval by the Change Authority or a scheduled CAB. These Changes will require the approval of an ECAB (Emergency Change Advisory Board) and State IT leadership following mutually agreed upon service change procedures.

User means, with respect to a Managed Application, an individual or entity that accesses such Managed Application.

WC means WebCenter.

WebLogic is a tool used to build and deploy enterprise Java EE applications.

22. SERVICE LEVEL AGREEMENTS, INCLUDING SERVICE LEVEL CREDITS

Contractor and the State agree that the service level agreements applicable to the Managed Applications that fall within the Contractor's scope of work and responsibilities as well as the corresponding service level credits, each as described in Exhibit 2 to this Attachment A, shall apply.

23. THIRD PARTY COOPERATION

The State may hire an independent, third-party "independent verification and validation" ("IV&V) contractor to assist with auditing the software and written deliverables, including the Project Management Plan and Acceptance criteria. The State may hire other independent contractors as it may require in order to assist with the project. Contractor will cooperate with requests of the State and the third party, including provision of: (i) written Documentation solely in support of HSEP M&O Services under this Contract as reasonably requested by the State; (ii) commercially reasonable assistance and support services to such third party; and (iii) reasonable access to Contractor as necessary for such third parties to perform their work. For Contractor to cooperate, third parties shall comply with Contractor's reasonable requirements regarding confidentiality, operations, standards, and security. Contractor shall support and maintain such third-party work product, provided the service provider complies with any Documentation applicable to Contractor in respect of the Services involved. The Contractor will be required to work with, provide access for, and collaborate with any third party the State brings in to assist in certification and/or audits.

Contractor will work collaboratively to maintain and grow relationships with State's Third-Party Vendors including DDI vendors, in order to efficiently deliver the M&O Services and meet the SLAs that are the subject of this Contract.

24. STAFFING and WORK LOCATION

Contractor Personnel will be properly educated, trained and qualified for the HSEP M&O Services they are to perform, and Contractor will put appropriate training in place to meet initial and ongoing training requirements of Contractor Personnel assigned to perform HSEP M&O Services.

1. Contractor shall be responsible, at its own cost and expense, for any and all recruitment, hiring, Contractor-specific training, education and orientation for all Contractor Personnel assigned or to be assigned to perform HSEP M&O Services or support the Requirements.
2. All Contractor Personnel, in addition to any Contractor security policies and procedures, shall be required to comply with the security requirements in this Contract.
3. Prior to accessing the HSEP Managed Applications, Contractor Personnel must undergo Pre-Employment Background Verification and Background Checks in accordance with the UnitedHealth Group policies which have been delivered to the State under separate cover. Further, all Contractor Personnel shall be subject to the policies of UnitedHealth Group relating to Annual Background Checks, US and Employee Sanctions Monitoring delivered to the State under separate cover. Contract shall provide written notification to the State as soon as practicable, of any modifications to these policies.
4. No Contractor Personnel will be placed on the project when a felony conviction is present that involves a crime against a person; a crime involving the use or misuse of computer network; a crime involving weapons, explosives or arson; a crime involving trade

secret/proprietary information; a crime involving theft, dishonesty, embezzlement, breach of fiduciary duty, identity theft, or other financial-related crimes, or a crime involving the sale or distribution of illegal drugs and/or controlled substances.

5. All Contractor employees providing or assigned to provide HSEP M&O Services or otherwise in a position to obtain or have access to State Information, shall execute a non-disclosure agreement in a form acceptable to the State.
6. The timing for transfer, reassignment or replacement of Contractor Personnel will be coordinated with requirements for timing and other elements of the HSEP M&O Services so as to maintain continuity in the performance of the HSEP M&O Services and avoid interruption or disruption to the Services.
7. Contractor will be solely responsible to provide workspace for Contractor's staff and Contractor's approved subcontractors in Chittenden County in the State of Vermont, to the extent that this Contract specifies staff to be based in Vermont. The Parties agree that Contractor will also employ staff outside of Vermont and outside the United States. Contractor shall provide State with an annual updated organizational chart including work locations of staff.

25. REQUEST SERVICES

This section sets forth the procedures for creating and handling requests for modifications to the Managed Applications. Such requests may include Discretionary and Non-Discretionary Service Requests.

(1) Service Requests Creation, Review and Approval

A. Either Contractor or State (through a State Representative) may, from time to time during the Term, request that Contractor develop or implement modifications to the Managed Applications by creating and submitting a Service Request, using the mutually agreed upon form, in the Ticket Management System.

B. Contractor shall review and update each Service Request to classify it as either a Discretionary Service Request or a Non-Discretionary Service Request. See paragraph C. below for the Discretionary Service Request review and approval process. See paragraph D below for the Non-Discretionary Service Request review and approval process.

C. Once a request is identified as a Discretionary Service Request and the State elects to pursue it, the request shall be added to the Change Request Log by the State and managed via the Operational Change Request Process referenced in Section 17 of this Attachment A. Once a Change Request has been approved or rejected, the State shall, as soon as reasonably practicable and in any event not more than five business days, update the associated Discretionary Service Request to reflect the decision. It is understood and agreed by the Parties that the Maximum Amount set forth in Section 3 on page 1 of this Contract and further referenced in Attachment B Section 9.2 includes funds specifically reserved and allocated to pay for Discretionary Service Requests. If and when this reserved amount is exhausted, no further Discretionary Service Requests will be approved, unless and until the parties execute an amendment to the Contract to increase the Maximum Amount and the amount allocated for Discretionary Service Requests.

D. Once a request is identified as a Non-Discretionary Service Request the Contractor shall make any other necessary changes and additions to the Service Request. State shall review the revised Service Request and, as soon as reasonably practicable and in any event not more than five business days after receipt of the revised Service Request, shall:

1. Approve the Non-Discretionary Service Request in the Ticket Management System;

2. Withdraw/Close the Non-Discretionary Service Request in the Ticket Management System, in which case no further action shall be taken in respect of the Service Request; or

3. Request that State and Contractor discuss the Service Request, in which case the Parties shall gather any necessary information and/or Contractor shall prepare a revised version of the relevant Non-Discretionary Service Request, until such time as a final decision to approve, withdraw, or close the Non-Discretionary Service Request is made by the Parties.

(2) **Effectiveness of a Service Request**

Contractor shall not commence performance of any services, functions or responsibilities set forth in a Service Request until approved in the Ticket Management System. Subject to paragraph (1)(C) above, if a Discretionary Service Request is approved in the Ticket Management System by both Parties, it shall constitute an approved and executed Change Request.

(3) **Service Request Services**

Contractor and State shall perform those services, functions and responsibilities identified as their respective responsibilities in the Request Services Functional Area of the requirements table in Exhibit 1.

26. PREMIUM PROCESSING DEVELOPMENT

Contractor shall support the State’s development of end-to-end integration functionality for transition of Qualified Health Plan (QHP) premium processing to insurance carriers beginning with coverage year 2022. Contractor shall perform the services described in this Contract on a time and material basis. These time and material services will be performed as requested and under the direction of the State according to the terms in Attachment B through September 30, 2021.

Due to State resource availability and the evolving COVID-19 pandemic the State postponed implementation from 2020 to 2021 in support of plan year 2022 instead of plan year 2021. In collaboration with the State, Contractor distributed both in-flight and planned workstream timelines that extend through the remainder of the project timeline to deliver a high quality, robust solution and allow for thorough operational readiness planning.

The State subsequently re-wrote the approved software requirements to adhere with best practices for CMS traceability. The Contractor will use the originally approved requirements when performing System Integration Testing (SIT) and the State will use the rewritten requirements to perform User Acceptance Testing (UAT). To reduce project risk associated with these two different sets of requirements, State added scope for the Contractor to review and analyze differences between the two sets of requirements, and it adds new State responsibilities to support this effort. The ALM Software will serve as the sole system of record for requirement analysis.

26.1 Premium Processing Scope

Contractor shall:

a) Participate in requirement identification, analysis, and functional design pertaining to the future-state functionality for QHP premium processing through electronic data interchange (EDI) transactions;

b) Participate in the definition of the technical solution and detailed system requirements for integrating Vermont Health Connect (VHC) with insurance carriers through EDI transactions for QHP premium processing;

c) Provide development support for the VHC transition of QHP premium processing to insurance carriers from WEX Health, including the following activities:

   i. Decoupling of WEX pay pages for QHP customers;
   ii. Re-direction of QHP customers to carrier pay pages;
   iii. Decoupling enrollment integration logic into multiple parts;
   iv. Updating business workflows for QHP and Mixed Households, and maintaining Medicaid workflows;
   v. Updates to VHC system jobs and system workflows;
   vi. Updates to WEX Health payment artifacts and relevant triggering points in current business workflows;
   vii. Re-alignment of reconciliation process for carrier data;
   viii. Creation of new interfaces and updates to existing interfaces with proper error handling;
   ix. Payment process changes for Vermont Premium Assistance (VPA) and Vermont Cost Share Reduction (VCSR) and associated Siebel, service-oriented architecture (SOA), and the enrollment change engine modifications;
   x. Carrier initiated non-payment terminations and reinstatements protocols; and
   xi. Business logic and integrations for legacy QHP and mixed household balances owed.

d) Provide Quality Assurance (QA) support for test case definition and execution related to user/system functionality and external integration points;

e) Ensure existing Medicaid billing processes are not impacted by changes to QHP and that Medicaid functional and business flows remain unchanged;

f) Attend weekly status meetings and provide weekly status reports detailing planned activities, tasks, start/finish dates;

g) Provide labor reports no less than every other week on the total hours expended per resource by week including resource billing role and rate;

h) Adhere to the Quality Assurance Surveillance Plan (QASP) for Section 26 Premium Processing Development (Exhibit 7), to include project management work practices, code delivery, and acceptance:

    i. Upon the State's written approval, the Contractor shall be made exempt from a QASP related activity provided the exemption is approved by the Department of Vermont Health Access (DVHA) Product Owner and DVHA Contract Owner;
    ii. Contractor shall adhere to all Contractor Deliverables noted in Exhibit 7, however, the Security Compliant deliverable is not tied to State's acceptance for Premium Processing Development;

i) Participate in generating diagram mapping of user workflows;
j) Participate in generating diagram mapping of system infrastructures including but not limited to updates to the Software Development Life Cycle (SDLC) document;
k) Provide integration updates required with WEX Health; and
l) Participate in performance testing as mutually agreed by the State and Contractor.
m) Perform a one-time analysis of the 178 re-written requirements provided by State including:
    i. Review of re-written requirements for clarity, consistency, and completeness;
    ii. Perform gap analysis against the original requirements to identify if the re-written requirements represent new functionality or present changes to the baseline functionality; and
    iii. Analyze mapping between re-written requirement and originally approved requirements.
n) Build an automated Requirements Traceability Matrix (RTM) report that can be executed by both SIT and UAT teams based on the ALM folder selected for the data source and extracts requirement documentation from ALM and populates it into a Microsoft Excel file according to a specification template provided by State.

26.2 Premium Processing Out of Scope

The following items and anything not expressly stated in Section 26.1 above are out-of-scope:

a) Triage of Incidents, Defects, or Problems within the State's infrastructure;
b) Training materials beyond what is needed for User Acceptance Testing; and
c) As a result of the one-time requirement gap analysis:
    i. Modifications to existing developed or approved features in re-written requirements and/or business rules; and
    ii. Gaps between the developed software solution and the previously approved software requirements will be considered defects and corrected as part of defect remediation efforts.

26.3 Premium Processing - State Responsibilities

State has provided a first draft of each of the below pre-requisites for Contractor to perform its requirements analysis and RTM development in accordance with Section 26.1.m and n. If pre-requisites do not meet the descriptions below, there may be risk to the project and additional effort may be required by the Contractor to complete the analysis:

a) Provide all re-written requirements in ALM, including all relevant support artifacts;
b) Provide the re-written requirements, including business rules, structured via hierarchical relationships defined for each ALM requirement in the requirement traceability metadata, so that no many-to-many relationships are present;
c) Provide a mapping of the re-written requirements back to the originally approved source ALM requirement number; and

d) Provide complete specification requirements for the RTM report that includes the data elements needed, content, layout, sorting, formatting, and sample data examples sufficient for development.

During the Contractor's requirement analysis and RTM development and until final execution of the Premium Processing Certificate of Acceptance, the State shall:

a) Facilitate and execute updates to the re-written ALM requirements based on Contractor's analysis to correct errors and omissions identified by Contractor's gap analysis, as mutually agreed upon by the State Product Owner and Contractor;

b) Update, formalize, and submit RTM to CMS;

c) Maintain records of the mapping from the re-written requirements, including business rules, back to the originally approved source ALM numbers; and

d) Not modify the originally approved or re-written requirements further unless it is mutually agreed to by the State Product Owner and Contractor.

EXHIBIT 1 – Contractor's Responsibilities by Functional Area.

For each Functional Area, Contractor shall perform the service requirements set forth in the following table. Any other functional area or requirement not clearly set forth in this Exhibit shall be deemed to not be within Contractor's scope of responsibility.

Functional Area	Sub Area	Req. #	Requirement
Application Maintenance and Operation Services	Adaptive Maintenance	**1.000**	Perform adaptive maintenance for the Managed Applications, including identifying, developing, testing, and implementing modifications to the Managed Applications to maintain usability.
Application Maintenance and Operation Services	Adaptive Maintenance	**1.001**	Coordinate performance testing with Third Party Vendors to determine whether performance of the Managed Applications has been affected by new upgrades to existing operating system, third party software Releases, or new or changed equipment, as required for Contractor to perform the Services.
Application Maintenance and Operation Services	Application Quality Assurance	**1.002**	Develop, document, implement, and manage QA processes and procedures for the delivery of the Application Maintenance & Operations Services that are within the scope of HSEP M&O Services.
Application Maintenance and Operation Services	Application Maintenance Tuning	**1.003**	Evaluate, identify, and recommend changes to enhance performance of the Managed Applications.
Application Maintenance and Operation Services	Application Maintenance Tuning	**1.004**	Perform application maintenance tuning to the Managed Applications to maintain agreed upon performance service levels as set forth in Exhibit 2.
Application Maintenance and Operation Services	Backup and Recovery Services	**1.005**	Provide data backup and recovery for data which is less than 4 days old and available within Oracle Recovery Manager (RMAN).

Functional Area	Sub Area	Req. #	Requirement
Application Maintenance and Operation Services	Configuration Management	**1.006**	Perform configuration management for components of all Managed Applications, which entails the identification, control, maintenance and verification of configuration items, the maintenance of the configuration management database, and report on configuration changes.
Application Maintenance and Operation Services	Corrective and Emergency Maintenance	**1.007**	Perform corrective and emergency maintenance, including the break/fix activities that enable the Managed Applications to provide the required functionality to meet applicable availability service levels as set forth in Exhibit 2.
Application Maintenance and Operation Services	Corrective and Emergency Maintenance	**1.008**	Resolve all incidents & problems within the scope of the Contractor's responsibilities impacting the Managed Applications entered into the contractually agreed ticketing system according to SLA and prioritization given by the State.
Application Maintenance and Operation Services	Database Administration and Support	**1.009**	Perform application data refreshes in lower environments as requested by State (excluding movement of Production data to lower environments).
Application Maintenance and Operation Services	Database Administration and Support	**1.010**	Implement database management in a manner required to support all agreed-upon Service Levels as set forth in Exhibit 2.
Application Maintenance and Operation Services	Database Administration and Support	**1.011**	Maintain databases that support the in-scope applications with a level of support that meets all agreed-upon Service Levels as set forth in Exhibit 2.
Application Maintenance and Operation Services	Database Administration and Support	**1.012**	Maintain and execute database archive processes and procedures as defined by and agreed-to by the State.
Application Maintenance and Operation Services	Database Administration and Support	**1.013**	Execute physical space management utilities on an as-needed basis to support agreed upon service levels as set forth in Exhibit 2.

Functional Area	Sub Area	Req. #	Requirement
Application Maintenance and Operation Services	Database Administration and Support	**1.014**	As needed for compliance with Service Levels as set forth in Exhibit 2, provide database administration and support for the Managed Applications. This support consists of monitoring and analyzing database activity; database performance tuning; maintaining all environment databases; documenting database-related settings, processes, and procedures for State system personnel; and certifying patches and advising whether they are required for State installations.
Application Maintenance and Operation Services	General Requirements	**1.015**	Contractor shall be responsible for providing Core M&O Services for the Managed Applications.
Application Maintenance and Operation Services	General Requirements	**1.016**	Contractor will maintain an Architecture Document to represent the current configuration standards of the Environment.
Application Maintenance and Operation Services	General Requirements	**1.017**	Contractor shall participate with the State in Lessons Learned Processes pertaining to M&O Services and Contractor will provide written content related to Contractor involvement.
Application Maintenance and Operation Services	General Requirements	**1.018**	Contractor shall update the State's System Design Document, which describes the system requirements, operating environment, system and subsystem architecture, files and database design, input formats, output layouts, human-machine interfaces, detailed design, processing logic, and external interfaces, with details of changes made to the above items by the Contractor and with documentation of changes made to the above items provided by the State.
Application Maintenance and Operation Services	Interface and Integration Support	**1.019**	Maintain, and document changes to, interfaces between the Managed Applications and other systems, in accordance with Contractor's responsibilities for the Managed Applications (as set forth in Attachment A, Section 6.1.1). Provide updated listing of certified interfaces.
Application Maintenance and	Interface and Integration Support	**1.020**	Contractor will work with AHS IT, BASU, VHC Operations and Third-Party Vendors to troubleshoot transmission issues. Contractor will work to identify causes, and

Functional Area	Sub Area	Req. #	Requirement
Operation Services			operational changes that will lead to successful data transmissions related to the scope of the Contractor's responsibilities based on SLAs as defined by Incident priority. Contractor will aid Third Parties in root cause analysis within the scope of this Contract.
Application Maintenance and Operation Services	Interface and Integration Support	**1.021**	Work with the State and other parties, as appropriate to maintain Interface Control Documents required to support the end-to-end Core M&O Service.
Application Maintenance and Operation Services	Interface and Integration Support	**1.022**	Test Managed Application interface changes, resolve compatibility issues, and track and report on compatibility issue resolution.
Application Maintenance and Operation Services	Interface and Integration Support	**1.023**	Monitor Managed Application interfaces as necessary to confirm that data transmissions to existing Third Party Vendors (including but not limited to payment vendors and carrier partners) are successful.
Application Maintenance and Operation Services	Interface and Integration Support	**1.024**	Perform data verification and reconciliation as required for reported Incidents in Contractor's ticketing system related to data transmissions to existing Third Party Systems.
Application Maintenance and Operation Services	Maintenance Services	**1.025**	Apply database patches.
Application Maintenance and Operation Services	Maintenance Services	**1.026**	Perform remedial maintenance as needed, which consists of performing database management system and application restarts.
Application Maintenance and Operation Services	Managed Application Support	**1.027**	Provide 24 X 7 Level 2 Support and Level 3 Support for Incidents that are initiated or initially detected inside or outside of State business hours dispatched from the Service Desk, provided that Level 3 Support shall be provided on an on-call basis outside of HSEP/VHC Business Hours of Operations and only for Priority Level 1 and Priority Level 2 Incidents.

Functional Area	Sub Area	Req. #	Requirement
Application Maintenance and Operation Services	Managed Application Support	**1.028**	Respond to business queries and ad hoc Non-Discretionary Service Requests related to M&O services.
Application Maintenance and Operation Services	Middleware Support Services	**1.029**	Provide maintenance and support for middleware and supporting utilities and perform middleware system recovery.
Application Maintenance and Operation Services	Middleware Support Services	**1.030**	Provide, install, configure and maintain middleware and associated components.
Application Maintenance and Operation Services	Middleware Support Services	**1.031**	Perform controlled stops and restarts to middleware servers as needed.
Application Maintenance and Operation Services	Middleware Support Services	**1.032**	Maintain middleware currency at Contractor-recommended patch levels.
Application Maintenance and Operation Services	Patch Management Services	**1.033**	Perform database management system, and other application Software patch deployment and patch management within system on the HSEP during scheduled Maintenance Windows.
Application Maintenance and Operation Services	Patch Management Services	**1.034**	Conduct all patch verification testing.
Application Maintenance and Operation Services	Performance and Capacity Planning and Management Services	**1.035**	Based on forecast information provided by State, identify and execute any required actions needed to maintain Availability of the Managed Applications in accordance with applicable Service Levels which are within the original nonfunctional system requirements.

Functional Area	Sub Area	Req. #	Requirement
Application Maintenance and Operation Services	Preventive Maintenance	**1.036**	Perform preventive maintenance to improve the efficiency and reliability of Managed Applications and minimize ongoing maintenance requirements.
Application Maintenance and Operation Services	Production Schedule Services	**1.037**	Provide job scheduling, job execution, reporting and Incident resolution.
Application Maintenance and Operation Services	Production Schedule Services	**1.038**	Implement and support current scheduling requirements, interdependencies, and rerun requirements for production jobs.
Application Maintenance and Operation Services	Production Schedule Services	**1.039**	Implement job scheduling requirements, interdependencies, State contacts, and rerun requirements for production jobs within the scope of the Contract.
Application Maintenance and Operation Services	Production Schedule Services	**1.040**	Prepare batch jobs for execution for Production and Non-production environments.
Application Maintenance and Operation Services	Production Schedule Services	**1.041**	Execute production batch jobs, in accordance with the defined Service Level Agreements, set forth in Exhibit 2.
Application Maintenance and Operation Services	Production Schedule Services	**1.042**	Provide quality control for reprocessing activities, such as batch reruns.
Application Maintenance and Operation Services	Release Services	**1.043**	Coordinate Release management with Third Party Vendors for Managed Application Releases within the Contractor's Release Entry Framework, including the distribution of updates/upgrades (e.g., new Releases, versions, service packs, patches, and Service Requests) to the Managed Applications.

Functional Area	Sub Area	Req. #	Requirement
Application Maintenance and Operation Services	Release Services	**1.044**	Plan and oversee the roll-out of Minor Releases of Managed Applications, including break-fix and Non-Discretionary Service Requests.
Availability Management	General Requirements	**1.045**	Investigate and remediate Incidents and Problems which impact Availability within the scope of the Contractor's responsibilities under this Contract.
Availability Management	General Requirements	**2.000**	The Availability Plan shall be reviewed and updated quarterly.
Availability Management	General Requirements	**2.001**	Contractor shall execute all activities within the Availability Plan.
Availability Management	General Requirements	**2.002**	Application servers shall prioritize work based on pre-defined rules and by monitoring actual run time performance statistics. Priority rules shall be specified in the application design documentation.
Availability Management	General Requirements	**2.003**	Document and publish the availability of the critical and high priority services that apply to the Contractor's Core M&O Services.
Availability Management	General Requirements	**2.004**	Contractor will utilize monitoring tools as part of Availability Management to identify actual or potential Incidents affecting availability and take action to prevent or minimize such impact. State must be notified when Incidents are identified affecting Environment Availability.
Capacity Management	General Requirements	**3.000**	A Capacity Plan shall be reviewed yearly and updated as required by the Contractor.
Capacity Management	General Requirements	**3.001**	Individual technology CIs (applications and databases) shall be monitored using an enterprise monitoring tool. Contractor shall review capacity/performance monitoring technology with State – Enterprise Architecture team prior to finalizing the Capacity Plan and prior to implementation.
Capacity Management	General Requirements	**3.002**	Contractor shall execute activities within the Capacity Plan.

Functional Area	Sub Area	Req. #	Requirement
Capacity Management	General Requirements	**3.003**	System shall support 300 concurrent internal and 200 external users (stateless connections). This shall be tested prior to go-live and periodically after Major Release and part of the Capacity plan.
DBMS & Clusterware Services	General Requirements	**4.000**	Contractor shall operate the DBMS and Clusterware infrastructure to meet the uptime expectations set forth herein.
DBMS & Clusterware Services	General Requirements	**4.001**	Perform controlled shutdowns and restarts as needed.
DBMS & Clusterware Services	General Requirements	**4.002**	Maintain currency at software vendor-recommended patch levels unless mutually agreed by State and Contractor.
DBMS & Clusterware Services	General Requirements	**4.003**	Perform continuous logging and monitoring of the DBMS and Clusterware infrastructure.
DBMS & Clusterware Services	General Requirements	**4.004**	Perform ongoing monitoring and tuning of Clusterware, DBMS servers, and databases to meet business performance requirements.
DBMS & Clusterware Services	General Requirements	**4.005**	Manage database level backups to meet State requirements and perform database restores as needed.
DBMS & Clusterware Services	General Requirements	**4.006**	Perform DBMS and Clusterware application level recovery as needed.
DBMS & Clusterware Services	General Requirements	**4.007**	Manage and monitor database replication to the DR environment.
DBMS & Clusterware Services	General Requirements	**4.008**	Provide maintenance and support for DBMS, Clusterware and supporting utilities.
DBMS & Clusterware Services	General Requirements	**4.009**	Perform Extract, Transform, and Load (ETL) and data migration operations.
DBMS & Clusterware Services	General Requirements	**4.010**	Perform database/schema changes to support application and environment changes.
DBMS & Clusterware Services	General Requirements	**4.011**	Manage Environment instance configurations with internal and external partners.

Functional Area	Sub Area	Req. #	Requirement
DBMS & Clusterware Services	General Requirements	**4.012**	Contractor will perform services, functions and responsibilities identified as their respective responsibilities with respect to the installation, configuration, and management of the DBMS and Clusterware infrastructure.
DBMS & Clusterware Services	General Requirements	**4.013**	The Contractor shall manage and perform database level backup, restores, and replication to the DR site.
DBMS & Clusterware Services	General Requirements	**4.014**	The Contractor shall support the troubleshooting, monitoring and usage of the DBMS and Clusterware infrastructure.
DBMS & Clusterware Services	General Requirements	**4.015**	The Contractor shall participate in the governance and change management process.
DBMS & Clusterware Services	General Requirements	**4.016**	Notification alerts will be sent when free space reaches specific levels (e.g. 25%, 20%, 15%, 10% …).
DBMS & Clusterware Services	General Requirements	**4.017**	Install, configure, and maintain DBMS, Clusterware and associated components.
DBMS & Clusterware Services	General Requirements	**4.018**	Manage and monitor Service Level Agreements (SLAs) which includes availability, reliability, throughput, and capacity of the databases.
DBMS & Clusterware Services	General Requirements	**4.019**	Perform database failover and failback operations as part of DR events.
Disaster Recovery Services	General Requirements	**5.000**	Maintain a State-specific Application Recovery and Application Validation procedures in support of a disaster recovery plan for the HSEP M&O Services (“Disaster Recovery Plan”) and provide such documents to State for review on an annual basis.
Disaster Recovery Services	General Requirements	**5.001**	Update the Application Recovery and Application Validation procedure sections of the Disaster Recovery Plan as required, including incorporating applicable test findings.
Disaster Recovery Services	General Requirements	**5.002**	The Contractor’s Business Continuity Plan, Service Continuity and restoration procedures, contact information, Architecture Documentation and Configuration information will have stored copies and/or access at redundant locations such that they are

Functional Area	Sub Area	Req. #	Requirement
			readily accessible in the event Contractor and/or State are unable to gain normal access.
Disaster Recovery Services	General Requirements	**5.003**	The Disaster Recovery Plan will include a risk assessment documenting and assessing the probability of risks to the Service(s) in scope.
Disaster Recovery Services	General Requirements	**5.004**	The Contractor is responsible for executing activities in the Disaster Recovery Plan which are identified in the plan as being the responsibility of the Contractor.
Reserved		**5.005**	
Disaster Recovery Services	General Requirements	**5.006**	Assist the Hosting Vendor in the Disaster Declaration process providing technical guidance relative to outage impact, developing and maintaining the decision, activation and notification process with State per the DR Plan.
Disaster Recovery Services	General Requirements	**5.007**	Following declaration of a Disaster, restore the Applications and validate the Applications are functioning once the hosted systems and supporting infrastructure is recovered by the Hosting Vendor in support of the applicable RTOs and RPOs set forth in the Disaster Recovery Plan as documented by the Hosting Vendor. In addition, work with Hosting Service Provider to remediate issues discovered with dependent infrastructure, data restoration, network and other technology relative to service restoration within the applicable RTOs and RPOs.
Disaster Recovery Services	General Requirements	**5.008**	Contractor shall update and maintain procedures for Application Recovery and Application Validation in support of the Disaster Recovery Plans for the HSEP based on the assumption that the HSEP's data will be recovered at an alternate data center that is approved by the State. This plan shall be under Change control and updated upon significant changes to services.

Functional Area	Sub Area	Req. #	Requirement
RESERVED		**5.009**	
Disaster Recovery Services	General Requirements	**5.010**	Contractor shall perform DR test annually as set forth in the DR Plan.
Disaster Recovery Services	General Requirements	**5.011**	Contractor shall include within the DR Plan, a process for application restoration back to normal/primary operations.
Disaster Recovery Services	General Requirements	**5.012**	Contractor shall work with Hosting Service Provider to remediate issues discovered with dependent infrastructure, data restoration, network and other technology relative to service restoration within the applicable RTOs and RPOs.
Disaster Recovery Services	General Requirements	**5.013**	The Disaster Recovery Plan will be under Change Management control.
Enterprise Content Management Services	General Requirements	**6.000**	Confirm proper operation of the ECM infrastructure.
Enterprise Content Management Services	General Requirements	**6.001**	Support and resolve issues elevated from ADPC, BASU & AHS IT for problems encountered using deployed capabilities of ECM architecture (WC, provisioning, authentication, Fed Cloud access).
Enterprise Content Management Services	General Requirements	**6.002**	Perform schema changes to support application and environment changes.
Enterprise Content Management Services	General Requirements	**6.003**	Participate in maturity of ECM Governance, managed by the State.
Enterprise Content Management Services	General Requirements	**6.004**	Provide maintenance and support for middleware and supporting utilities, perform middleware system recovery, and perform controlled stops and restarts to ECM servers as needed.

Functional Area	Sub Area	Req. #	Requirement
Enterprise Content Management Services	General Requirements	**6.005**	Contractor shall perform those services, functions and responsibilities identified as their respective responsibilities with respect to the installation, configuration, and management of the Enterprise Content Management (ECM).
Enterprise Content Management Services	General Requirements	**6.006**	The Contractor shall participate in governance and change management process.
Enterprise Content Management Services	General Requirements	**6.007**	Provide, install, configure, maintain, and monitor availability, reliability, and performance of ECM for OEM (WebCenter (WC) Suite, WC Capture, WC Recognition, WC Content, WC Capture Server, WC Recognition Server, WebCenter Content Server, Web Logic Server, SFTP Server, Database, SOA Connection and WebUI at Contractor recommended patch levels to meet business performance requirements.
Enterprise Content Management Services	General Requirements	**6.008**	Maintain and operate the five instance configurations (Development, Test, Training, Stage, and Production), for ECM, including the maintenance and operation of a mechanism by which external partners can send content into the ECM.
Enterprise Content Management Services	General Requirements	**6.009**	ECM Monitoring: • Manage and monitor SLAs including availability, reliability, throughput, and capacity. • Perform logging and Monitoring of ECM Infrastructure. • Maintain the service composites. • Perform runtime Service Usage Tracking, Monitoring, Alert Notifications, and Exception Management. • Maintain Federal Cloud connectivity.
Enterprise Content Management Services	General Requirements	**6.010**	Error Logs for WC maintained and reviewed and reviewed on a daily recurring frequency.
Enterprise Content Management Services	General Requirements	**6.011**	Run and maintain the daily scripts to produce daily WC reporting.

Functional Area	Sub Area	Req. #	Requirement
Enterprise Content Management Services	General Requirements	**6.012**	Maintain ECM error log, perform reviews of logs and manage error log email-distribution list.
Enterprise Content Management Services	General Requirements	**6.013**	Perform failover and failback operations as part of scheduled and unscheduled DR events.
Enterprise Content Management Services	General Requirements	**6.014**	The Contractor shall support the troubleshooting, monitoring and usage of the ECM infrastructure.
Escalation Management	General Requirements	**7.000**	Generate the following notifications for all high priority Incidents: initial notification, update notification(s) and restored/summary notification.
Escalation Management	General Requirements	**7.001**	Use a standard impact communication template for priority 1 and 2 Incidents and work with State to improve on a go forward basis.
Escalation Management	General Requirements	**7.002**	Follow internal escalation process for Managed Applications.
Escalation Management	General Requirements	**7.003**	Follow external escalation process for Managed Applications.
Event Management / Monitoring	General Requirements	**8.000**	The Contractor shall implement database and application protection capabilities to detect and eliminate malicious software and/or unauthorized external connection attempts.
Event Management / Monitoring	General Requirements	**8.001**	Contractor will install Contractor's tools on Servers within the HSEP environment that enable monitoring and management capabilities, depending upon the State's contract with the Hosting Service Provider
Event Management / Monitoring	General Requirements	**8.002**	Application logs and error messages shall be monitored by the Contractor. Appropriate action shall be taken by integrating with ITSM.
Event Management / Monitoring	General Requirements	**8.003**	The Contractor must maintain a monitoring plan for the technology it is directly accountable for delivering. The plan must include the accountable individual/team, strategy for monitoring, tools used, thresholds, trends and baselines used, monitoring intervals and calculations for alerting and reporting.

Functional Area	Sub Area	Req. #	Requirement
Event Management / Monitoring	General Requirements	**8.004**	The Contractor must present a strategy for correlating monitoring events and alerts and promptly create Incidents for "actionable" alerts that may impact the service in any way. Such Incidents must be raised proactively regardless of whether symptoms have been noticed by users of the system.
Event Management / Monitoring	General Requirements	**8.005**	Contractor shall work with the State's third parties and DDI providers to collect user experience management ("UEM") monitoring requirements and then deploy the appropriate UEM strategy based upon the requirements. Requirements shall be mutually agreed by both Contractor and State prior to UEM solution deployment (i.e. Dynatrace is the primary tool used for UEM).
Event Management / Monitoring	General Requirements	**8.006**	Contractor shall trend the UEM performance over 60 days to determine an operational baseline during peak (open enrollment) and non-peak periods. The baseline shall be used by the Contractor for both alerting and reporting to the State.
Event Management / Monitoring	General Requirements	**8.007**	An Event Management plan shall be created by the Contractor, reviewed at least annually with the State, and updated as required by the Contractor.
Event Management / Monitoring	General Requirements	**8.008**	Contractor shall provide Application Performance Monitoring and Management capabilities (i.e. transaction monitoring, synthetic transactions, component root cause analysis (e.g. Application Server Management) but solely for the Managed Applications as part of the M&O Core Services. Details for monitoring must be supplied to State for approval and during periodic service reviews. Details shall include: • Tools utilized; • Monitoring location(s); • Synthetic transactions utilized; and • Calculations used to determine thresholds, alerts, baselines and service reports.
Event Management / Monitoring	General Requirements	**8.009**	Contractor shall provide transaction tracking and log consolidation capabilities across all technology managed by the Contractor (i.e. current Contractor utilizes the following tools: HP Ops manager, HP Openview, HPPM, Dynatrace, VMWare vSphere, Splunk, and OEM)

Functional Area	Sub Area	Req. #	Requirement
Event Management / Monitoring	General Requirements	**8.010**	Monitoring and diagnostic services shall be configured by Contractor to access monitoring and diagnostic data collected. The data collected shall include information, warning, errors, threshold violations, and other pertinent information about the operation and health of the application that are within the scope of M&O Services for the Managed Applications. Contractor will provide reports and access to raw data to State upon request.
Event Management / Monitoring	General Requirements	**8.011**	Contractor will be accountable for the configuration of application monitoring tools specified for use or deployment within the Event Management Plan.
Event Management / Monitoring	General Requirements	**8.012**	Contractor will monitor the Services by utilizing the tools, methods, and approach specified in the Event Management Plan.
Event Management / Monitoring	General Requirements	**8.013**	Contractor shall validate that alerts from the monitoring tools are labeled to indicate Severity of the application events. Events are classified as Critical, Major, Warning, Informational, as an example. Incident Management System clearly posts correct event severity during integration.
Event Management / Monitoring	General Requirements	**8.014**	Contractor will report outages and service interruptions when identified. Incident tickets and escalations will be raised to cause investigation and remediation to commence with Third Party Contractors when applicable. Contractor will communicate status and progress during the outage or service interruption when applicable as provided by the Third-Party Contractor using the methods and according to the frequency specified in the Event Management Plan.
Event Management / Monitoring	General Requirements	**8.015**	Contractor shall make use of technology that provides end-to-end monitoring of real-time transactions for Managed Applications inclusive of user experience management (UEM). The solution must be able to dissect and visualize transaction flows, loads and response times through all the transactional tiers (e.g. web request, web tier, application tier, and database tier). The end-to-end monitoring tool must be able to log and view user actions and have drill down capability to examine service-side code within the scope of Managed Applications.

Functional Area	Sub Area	Req. #	Requirement
Event Management / Monitoring	General Requirements	**8.016**	Contractor must make use of the selected monitoring technology 24x7x365 within Production ("LIVE") and as requested by the State and within Staging during testing. The Contractor shall support the initiatives of the DDI team(s) by utilizing this tool for both proactive (testing and daily analysis) in production as well as reactive (to trouble shoot code and performance issues reported in Contractor's ticketing system). Contractor shall share performance, analysis, and validation results with agreed State personnel and third parties.
Identity & Access Management Services	General Requirements	**9.000**	Confirm proper operation of the IAM infrastructure.
Identity & Access Management Services	General Requirements	**9.001**	Maintain middleware currency at Contractor-recommended patch levels.
Identity & Access Management Services	General Requirements	**9.002**	Provide maintenance and support for middleware and supporting utilities and perform middleware system recovery.
Identity & Access Management Services	General Requirements	**9.003**	Perform controlled stops and restarts to middleware servers as needed.
Identity & Access Management Services	General Requirements	**9.004**	IAM Monitoring: • Logging and Monitoring of IAM Infrastructure (OIM, OAM, OAAM, SOA, OVD, OUD, load balancer, WebLogic, JVM, JDBC, JCA) with tools such as OEM and Splunk. • Monitor events in OIM for issues related to user registration and provisioning. Runtime Service Usage Tracking, Monitoring, Alert Notifications, and Exception Management.

Functional Area	Sub Area	Req. #	Requirement
Identity & Access Management Services	General Requirements	**9.005**	Performance: • Meet business performance requirements of throughput and capacity. • Conduct regular capacity planning of the IAM components in all environments and adjust infrastructure sizing as needed • Confirm IAM components remain integrated with Managed Applications during normal operations and upgrades (excludes major upgrades which shall be handled by DDI).
Identity & Access Management Services	General Requirements	**9.006**	Manage and control code and files related to customizations and configuration changes of IAM components.
Identity & Access Management Services	General Requirements	**9.007**	Support and resolve issues elevated from BASU & AHS IT for problems encountered using deployed capabilities of the IAM architecture (registration, provisioning, authentication, etc.).
Identity & Access Management Services	General Requirements	**9.008**	Participate in maturity of IAM Governance, managed by the State.
Identity & Access Management Services	General Requirements	**9.009**	Manage Environment instance configurations with internal and external partners.
Identity & Access Management Services	General Requirements	**9.010**	Contractor shall perform those services, functions and responsibilities identified as their respective responsibilities with respect to the installation, configuration, and management of the IAM infrastructure, which will enable the management, authentication, and authorization of users.
Identity & Access Management Services	General Requirements	**9.011**	The Contractor shall confirm proper security and compliance to industry and Vermont standards.
Identity & Access Management Services	General Requirements	**9.012**	The Contractor shall support the troubleshooting, monitoring and usage of the IAM infrastructure.

Functional Area	Sub Area	Req. #	Requirement
Identity & Access Management Services	General Requirements	**9.013**	The Contractor shall participate in governance and change management process.
Identity & Access Management Services	General Requirements	**9.014**	Provide, install, configure, and maintain middleware and associated components. (OIM, OAM, OAAM, OVD, OUD, SOA Suite (for OIM), OEM, Web Logic Server, OHS).
Identity & Access Management Services	General Requirements	**9.015**	Manage and control documentation on customizations and configuration changes of IAM components.
Knowledge Management	General Requirements	**10.000**	Establish and maintain a knowledge repository.
Knowledge Management	General Requirements	**10.001**	Define workflow, including editing, review and approvals for creation of knowledge artifacts.
Release Management	General Requirements	**12.000**	Each pre-production release shall include the following: • Release-specific hardware and Managed Application components. • Detailed hardware and software configuration information including any software and hardware dependencies and instructions at a level of detail that will enable administrator's staff to rebuild and configure the hardware environment without outside assistance. • Detailed configuration information for any 3rd party hardware and software. Vendor shall provide updated documentation when upgrades to software or equipment occurs.
Release Management	General Requirements	**12.001**	Contractor will assist State as required in preparing State desktops, networks and other infrastructure and applications if integration to State technology is required. Contractor must also provide documentation that includes configuration document, release notes, FAQs and others that outline acceptable desktop, laptop, mobile versions, browser versions, operating system requirements and other configuration details as required.
Release Management	General Requirements	**12.002**	Contractor shall provide access for appropriate and authorized State team members to the test and training environments to confirm correct implementation of

Functional Area	Sub Area	Req. #	Requirement
			changes before the changes are released to the production environment.
Release Management	General Requirements	**12.003**	Project teams (Contractor-supplied or otherwise) shall maintain an automated process for purging temporary files when necessary.
Release Management	General Requirements	**12.004**	Contractor shall provide the required system permissions, documentation and training that describe the procedures for Third Party Contractors to add, update or remove user IDs and passwords. When a request to State for adding/deleting/modifying a user account is requested, Contractor shall support State to complete the task.
Release Management	General Requirements	**12.005**	Contractor will confirm the system includes supported releases of all software, including any third-party application components. Documentation shall be presented to Change Mgt., as part of the production change ticket.
Release Management	General Requirements	**12.006**	Contractor shall validate that each interface is working correctly. Project teams (Contractor-supplied or otherwise) will repair all interface-related problems caused by Contractor-developed interfaces.
Release Management	General Requirements	**12.007**	Contractor will utilize State requirements to maintain the State Environments and a Provisioning Release Plan. Contractor will then review the Provisioning Release Plan with the State. The Provisioning Release Plan will be under Change control and must be approved before any implementation.
Release Management	General Requirements	**12.008**	The Contractor shall coordinate with the State, and other Third Party Contractors as required, in advance of any release or changes to allow the HSEP team to adequately perform User Acceptance Testing (UAT), verify the release meets the requirements and needs of the business and train to support the smooth operation of the Managed Applications. Contractor will validate, where applicable within the scope of this Contract, the documenting of application changes and building training materials for end users, to include problem resolution, workarounds, updates and State requested changes.

Functional Area	Sub Area	Req. #	Requirement
Release Management	General Requirements	**12.009**	In the event that Contractor makes changes to an existing application or integration, Contractor shall perform unit and integration testing for the applications that the Contractor owns and external interfaces within the scope of this Contract. Unless otherwise approved by the State, Integration testing can only start after unit testing has completed. All requirements in the Release must have at least one Integration test scenario, and those must be reviewed and edited or approved by the state prior to execution. If defects, Incidents or Problems are discovered, the Contractor shall work with other Third Party Vendors and State to remediate the issue based upon the Project Schedule (for project defects), SLAs for Incidents and State prioritization for Problems. End-to-End definition can be found in the glossary section.
Release Management	General Requirements	**12.010**	Contractor will use automated deployment tools and techniques, where applicable, to build, manage and synchronize different environments.
Release Management	General Requirements	**12.011**	Contractor will support automated patch deployment.
Release Management	General Requirements	**12.012**	Contractor shall test and apply patches for Third Party Software products before release.
Release Management	General Requirements	**12.013**	Contractor shall update the HSEP's M&O Manual, when applicable, which will serve as an operator's instruction manual. It will include HSEP administration procedures and describe the operations of the production system. It will contain specific instructions on things an operator needs to do to manage the HSEP on a daily basis, descriptions of administrative tasks, instructions on how to run the job, and what to do in abnormal situations. This document shall become the property of State and shall be reviewed and approved upon completion.
Release Management	General Requirements	**12.014**	Contractor shall provide State designated support staff (help desk, call center, other) with help desk scripts, FAQs, support documents, known workarounds, procedures, work instructions and decision trees needed to provide service excellence. These documents shall become State property and stored within State's designated Knowledge Management system.

Functional Area	Sub Area	Req. #	Requirement
Release Management	Release Management	**12.015**	There is a unified Release process and Policy for the 'Common Platform'. Contractor shall participate in this process, which shall be governed by Change Control. Contractor shall coordinate with other Third-Party Vendors, as necessary, to coordinate and schedule Changes and Releases.
Request Services	Change Management Services	**13.000**	Change Management plans will be documented in a Change Management Plan by the Contractor that will conform to State's existing Change Management processes. It shall include the following components: • Integration plan with other processes (Incident, Problem, Release, Configuration). • Responsibility matrix (RACI). • Procedures and work instructions on how State and Contractor's staff shall utilize the Change Management ticketing system to log, manage, track and close production change tickets. • Utilization of Change Tasks to manage and track individual activities related to the change. Integration of these tasks with other parties as directed by State is mandatory and the plan must be documented. • Maintain transparency for all Changes in the system of record with State and other parties as directed by State.
Request Services	Change Management Services	**13.001**	Provide a mutually agreeable lead-time for developing transition activities inclusive of end-user notification, review, collaboration, integration, testing, training, documentation. This is applicable for all Changes to the HSEP environments developed or maintained by Contractor relative to applications, databases, middleware, utilities, policies, procedures, processes. State shall have final approval over whether enough time has been allotted for planned Changes.
Request Services	Change Management Services	**13.002**	Any required outages not following the Emergency Change sub-process must be scheduled and approved by the State 30-days in advance or by mutual agreement.
Request Services	Change Management Services	**13.003**	Work with State's change control board to plan and schedule strategic business and technology events that affect delivery of the service.

Functional Area	Sub Area	Req. #	Requirement
Request Services	Change Management Services	**13.004**	Create a production change control ticket for each Change and submit for approval in the Ticket Management System. Once approved in the Ticket Management System by both Parties, the Change Ticket shall constitute an approved and executed Change Request.
Request Services	Change Management Services	**13.005**	Follow mutually agreed upon Contractor's procedures to communicate Change activity to impacted stakeholders. Contractor shall make commercially reasonable efforts to inform State at least 48 hours prior to any Change activity that is expected to require or cause any Managed Application to be offline or unavailable.
Request Services	Change Management Services	**13.006**	Coordinate with State, Third Party Vendors and other third parties as needed with respect to execution of Changes that are within Contractor's scope of responsibility for Managed Applications.
Request Services	Change Management Services	**13.007**	Perform post deployment validation, which are checkouts to confirm Change is working as desired for Contractor developed changes per the State approved request.
Request Services	Change Management Services	**13.008**	Following Contractor's Change closure procedures, close the Change Ticket.
Request Services	Change Management Services	**13.009**	Work within State's existing Change Management processes. Contractor shall provide resources to attend CCB and OCRB meetings with appropriate decision makers to help State manage an effective Change processes for the State.
Request Services	Change Management Services	**13.010**	Assess each proposed change for its business and technical risk based upon mutually agreed criteria and weighting with State. Risks will be documented with the Change Management system of record through a production change ticket. The Change Risk level will trigger the level of assessment and approvals based upon State requirements and existing processes.
Request Services	Change Management Services	**13.011**	Schedule and log production change tickets against Service CIs within the Change Management system of record. These changes include modifications to infrastructure, applications, processes, policies, to minimize impact on the business.

Functional Area	Sub Area	Req. #	Requirement
Request Services	Change Management Services	**13.012**	Relate Incidents and Problems that require a Change with a production change ticket and track the production change ticket through completion. The Incident shall then be updated by the Contractor.
Request Services	Change Management Services	**13.013**	Contractor shall work to define standard changes and standard Non-Discretionary Service Requests. These are changes that are considered low risk and highly repetitive for pre-approval consideration. Contractor shall endeavor to include defined workflow and responsibility matrix (RACI) in each standard change and service request. Contractor shall be responsible for creating and maintaining this list of Standard Changes and associated SLAs within the mutually agreed Knowledge Management system. Once approved by State, the Contractor does not need approval to release the change but will still be required to log a production change ticket into the Change Management system.
Request Services	Change Management Services	**13.014**	Where applicable or mutually agreed upon Contractor is responsible for providing updated screenshots / updates to training material they created / train State trainers & testers in the event the requested change created by the Contractor falls under the Release Management requirements.
Request Services	Change Management Services	**13.015**	Contractor shall update architecture documents including information provided by Third Party Vendors when implementing changes to the HSEP. Updates must be approved via the Change Management process first.
Request Services	Change Management Services	**13.016**	Schedule downtime within common maintenance windows when possible. Outages outside the agreed maintenance windows must be coordinated and approved with other Platform providers and State and must consider integration points. Outages required outside the agreed maintenance windows must follow the Emergency Change Sub-process.
Request Services	Change Management Services	**13.017**	Notify State of all changes performed by Contractor's contracted Third-Party Vendors. As with other Changes to the system, third-party modifications and testing shall require a production change ticket and follow the Change Management Process.

Functional Area	Sub Area	Req. #	Requirement
Request Services	Change Management Services	**13.018**	Contractor shall assess the impact of all Changes or pending Changes of which it is aware, which affect the validity of the existing Disaster Recovery Plan. Contractor will update the DR Plan as needed to address such Changes. The Contractor shall review all proposed Changes to the Disaster Recovery Plan and the updated plan, with the State.
Request Services	Change Management Services	**13.019**	Emergency Changes will be reviewed and approved by a State designated Emergency Change Review Board prior to deploying emergency releases. Emergency Changes can only be submitted by the Contractor's designated agents. State owns and governs the Emergency Change Process and has final approval for releasing Emergency Changes into the system. Once the Emergency Change is approved by State, the Contractor must open and fully complete the production change associated with that ticket within 48 hours. Emergency Changes must be linked to an Incident.
Request Services	Change Management Services	**13.020**	Assign a Change Coordinator that is accountable for Contractor's interface with the Change Management process and so that the Contractor's production change tickets are being completed according to State standards and best practices. Contractor's Change Coordinator will also cooperate with State and other Third-Party Contractors to coordinate Change tasks. Change Coordinator is also responsible to bring relevant subject matter expertise to represent production change tickets at Change Management meetings.
Request Services	Change Management Services	**13.021**	Approved production change tickets will be placed on a Forward Schedule of Change (FSC). Contractor shall coordinate to confirm the FSC is up to date and accurate. Contractor shall share FSC with State at weekly OCRB meetings or as reasonably requested.
Request Services	Change Management Services	**13.022**	The unified Change Mgt. process shall include a designation for Changes that represent the introduction of new Service attributes or the significant change to existing Service attributes. Such Changes shall be managed under a separate sub-process that shall follow a standard Project Management methodology.

Functional Area	Sub Area	Req. #	Requirement
Request Services	Change Management Services	**13.023**	The production environment is managed under change management process.
Request Services	Incident Management Services	**13.024**	By implementing a workaround or through other means, restore the affected functionality of the Managed Applications with respect to each Incident that is within Contractor's Scope of responsibility for Managed Applications.
Request Services	Incident Management Services	**13.025**	Update Tickets in the Ticket Management System to reflect current status.
Request Services	Incident Management Services	**13.026**	Contractor shall execute applicable activities within the Incident and Problem Management processes.
Request Services	Incident Management Services	**13.027**	State has ultimate authority for determining ticket impact, urgency and priority in accordance with the criteria identified in Attachment A, Section 6.2.1 of this Contract. State also has ultimate authority to close tickets as required by the business. State will take necessary action to validate the ticket resolution or information needed to resolve the issue within 15-20 business days, otherwise, ticket will be closed by Contractor due to lack of information. Ticket Impact and Urgency may be upgraded or downgraded based upon changing circumstances and information. This upgraded/downgrade may be performed by the Contractor (with approval by State) or modified by State.
Request Services	Incident Management Services	**13.028**	Classify the Incident according to Priority Level with the State having final approval for that priority level.
Request Services	Incident Management Services	**13.029**	Investigate and diagnose the Incident.
Request Services	Incident Management Services	**13.030**	Coordinate with State, Third Party Contractors and other third parties as needed with respect to Incidents that are not within Contractor's Scope of responsibility for Managed Applications.
Request Services	Incident Management Services	**13.031**	Following an Incident's restoration, State shall close the Ticket upon State approval.

Functional Area	Sub Area	Req. #	Requirement
Request Services	Incident Management Services	**13.032**	Follow mutually agreed upon Contractor's procedures for Priority Level 1, Priority Level 2, Priority Level 3, and Priority Level 4 Incidents.
Request Services	Incident Management Services	**13.033**	Follow agreed upon procedures maintained by the State for Security Incidents.
Request Services	Incident Management Services	**13.034**	Communicate Incident status to State at the frequencies and to the individuals and offices in accordance with Contractor's procedures as defined in the SLAs found in Exhibit 2.
Request Services	Incident Management Services	**13.035**	Escalate Incidents in accordance with mutually agreed upon Contractor's procedures.
Request Services	Incident Management Services	**13.036**	An Incident and Problem Management processes shall be maintained as mutually agreed by State and Contractor that integrates with State's existing processes and tools. The Incident and Problem Management processes shall be reviewed on an ongoing basis and updated accordingly to meet the business needs. The processes shall be under the control of Change Management.
Request Services	Incident Management Services	**13.037**	State and approved Third Party Vendors shall have the ability to submit Incidents and have the ability to update/ modify tickets within the system of record.
Request Services	Incident Management Services	**13.038**	Tickets assigned to the Contractor shall be managed, tracked and monitored through resolution by the Contractor within the Contractor's ticketing system.
Request Services	Incident Management Services	**13.039**	Contractor shall coordinate and work with other providers, Third Party Contractors and State as necessary to diagnose and resolve Incidents and perform root cause analysis & resolutions for Problems regardless of the ticket priority.
Request Services	Incident Management Services	**13.040**	Resolution, workarounds for Incidents and Root Cause/resolution for all Problems shall be tracked and stored by the Contractor in a central ITSM System. Detailed location of any knowledge and/or workarounds shall be within the ITSM tool.
Request Services	Incident Management Services	**13.041**	The Contractor shall confirm that all workarounds to Incidents are retired upon Problem resolution. This shall be auditable within the Change Management process.

Functional Area	Sub Area	Req. #	Requirement
Request Services	Incident Management Services	**13.042**	Incident remediation and permanent fix is considered part of the Contractor's function and part of the service provided to State for its scope of responsibility within this Contract.
Request Services	Incident Management Services	**13.043**	Contractor shall assign an Incident and Problem Manager that is accountable for ensuring that issues are being actively managed and meet service level obligations and that the Service matches the functional and non-functional requirements. The Contractor shall meet with State to review Incidents based upon a schedule that meets the needs of the State. Incidents will be log into the designated ITSM System. Contractor will look to reduce Incident metrics with the goal of reducing the incoming trends.
Request Services	IT Service Management (ITSM) Services	**13.044**	Contractor will migrate open ticket data from the former ITSM System (current tool is HPSM) into the proposed ITSM System for historical purposes.
Request Services	IT Service Management (ITSM) Services	**13.045**	Contractor will provide services for exporting open ticket data from current ITSM System in a State-agreed format (e.g. full relational database backup) and a complete data dictionary upon Contract termination.
Request Services	IT Service Management (ITSM) Services	**13.046**	The ITSM System shall provide the State the capability for opening, tracking and updating tickets through closure based on a mutually agreed upon process. The in-scope ITSM processes are: • Incident, Problem and Change Management, inclusive of the following: • Change Requests/Orders originating from CCB; • Changes reviewed and approved at OCRB; and • Request Fulfillment.
Request Services	IT Service Management (ITSM) Services	**13.047**	The ITSM System shall provide access to State and Contractor 24 x 7 x 365.
Request Services	IT Service Management (ITSM) Services	**13.048**	The ITSM System shall support the State agreed ITSM processes and requirements as documented in this Contract.
Request Services	IT Service Management	**13.049**	Contractor shall provide encryption via HTTPS / TLS for access to the ITSM System.

Functional Area	Sub Area	Req. #	Requirement
	(ITSM) Services		
Request Services	IT Service Management (ITSM) Services	**13.050**	Contractor shall provide the ability for the State to authorize State users' access to ITSM that should be added, removed, or modified.
Request Services	IT Service Management (ITSM) Services	**13.051**	Contractor shall provide the State the capability to add, update and modify Incident tickets within the ITSM System and add/remove attachments to Incidents.
Request Services	IT Service Management (ITSM) Services	**13.052**	Contractor shall support the capability for the State to submit Incident and Change tickets within the Contractor's ticketing system and be able to view and report on both opened and closed tickets and the following details: status, priority, ticket details, history and work notes, reporting SR #, release number resolution is dependent on.
Request Services	IT Service Management (ITSM) Services	**13.053**	Contractor shall provide the capability for the State to log requests into the ITSM System of record.
Request Services	IT Service Management (ITSM) Services	**13.054**	Contractor shall use the ITSM System as the single source for all in-scope ITSM processes and provide transparency to the State of status of tickets and timely closure per SLAs as defined in Exhibit 2
Request Services	IT Service Management (ITSM) Services	**13.055**	Contractor shall configure mutually agreed notifications into the ITSM System for updates to tickets and requests throughout the lifecycle of the ticket.
Request Services	IT Service Management (ITSM) Services	**13.056**	The Problem ticket managed by the Contractor shall track workarounds through retirement of that workaround, closure of the Problem ticket and tracking release of the permanent fix to the proposed delivery date.
Request Services	IT Service Management (ITSM) Services	**13.057**	When possible, the Contractor shall require the root-cause of the Problem to be documented by the responsible vendor within the ITSM System for State review prior to closure.

Functional Area	Sub Area	Req. #	Requirement
Request Services	IT Service Management (ITSM) Services	**13.058**	Contractor shall support the capability for the State to review Problem tickets within the Contractor's ticketing system for both opened and closed tickets and their details including status, priority, ticket details, and history and work notes.
Request Services	IT Service Management (ITSM) Services	**13.059**	The ITSM System shall provide the State the capability to search for tickets within the ITSM System regardless of the state of the ticket (e.g. opened, closed) or the submitter of the ticket.
Request Services	IT Service Management (ITSM) Services	**13.060**	Contractor shall provide the State the capability to approve Service Changes within the ITSM System interface or via an email that updates the ITSM System and that supports the documented process.
Request Services	IT Service Management (ITSM) Services	**13.061**	Contractor and State shall work together to make or submit recommendations to enhance the features and functions of the ITSM solution.
Request Services	IT Service Management (ITSM) Services	**13.062**	Contractor shall provide State access to the ITSM System through a mutually agreed browser.
Request Services	IT Service Management (ITSM) Services	**13.063**	Contractor shall provide the State the capability to add and remove attachments to Incident tickets within the ITSM System.
Request Services	IT Service Management (ITSM) Services	**13.064**	For incidents that the Contractor is responsible for resolving, Contractor shall complete the resolution field of the Incident for review by the State prior to closing the Incident.
Request Services	IT Service Management (ITSM) Services	**13.065**	Contractor will provide and maintain on-demand access to all data from current ITSM System for 3 months beyond expiry of services Contract.
Request Services	Problem Management Services	**13.066**	Create a Problem Ticket as needed to manage the root cause analysis and solution implementation for multiple Incidents.
Request Services	Problem Management Services	**13.067**	For each Priority Level 1 and 2 Incident that requires a Problem Ticket, Contractor will create a Problem Ticket and assign it to an Incident manager.
Request Services	Problem Management Services	**13.068**	Classify the Problem according to Priority Level as defined in Attachment A, Section 21, Defined Terms

Functional Area	Sub Area	Req. #	Requirement
			with the State having final approval for that priority level.
Request Services	Problem Management Services	**13.069**	Perform analysis to identify the underlying root cause of the Problem and of any Incidents caused by the Problem within the scope of the Contractor's responsibilities in this Contract.
Request Services	Problem Management Services	**13.070**	Assign an Incident manager for each Priority Level 1 and 2 Problem to investigate root cause and to manage the Problem Ticket according to the Problem Management process for those Problems within the Core M&O Services scope of this Contract.
Request Services	Problem Management Services	**13.071**	Coordinate with State, Third Party Vendors and other third parties as needed with respect to Problems that are within Contractor's Scope of responsibility for Managed Applications.
Request Services	Problem Management Services	**13.072**	Contractor shall work with State and designated Third Parties to jointly perform root cause analysis and resolve problems as defined in the SLAs as set forth in Exhibit 2.
Request Services	Problem Management Services	**13.073**	After root cause of a Problem has been identified by Contractor, the Contractor will communicate the estimated remediation plan effort and coordinate execution of a plan for eliminating the potential risk of future Incidents resulting from the Problem for the Managed Applications impacted with BASU, AHS IT, ADS Security and VHC Operations management within the scope of M&O Services provided in this Contract.
Request Services	Problem Management Services	**13.074**	Follow State's procedures for consulting with SME stakeholders as needed to resolve problems.
Request Services	Problem Management Services	**13.075**	Follow Contractor's procedures for closing the Problem Ticket when it has been resolved.
Request Services	Problem Management Services	**13.076**	Communicate Problem status to State at the frequencies and to the individuals and offices in accordance with mutually agreed upon Contractor's procedures as defined in SLAs.
Request Services	Problem Management Services	**13.077**	Escalate Problem investigation in accordance with mutually agreed upon Contractor's procedures.

Functional Area	Sub Area	Req. #	Requirement
Request Services	Problem Management Services	**13.078**	Update Problem Tickets in the Ticket Management System to reflect current status.
Request Services	Problem Management Services	**13.079**	Monitor and prioritize inactive Problem Tickets if it is determined that further investigation should not continue due to lack of business prioritization or lack of cost benefit.
Request Services	Service Desk Services	**13.080**	Use the ITSM tool ServiceNow tool as the single point of contact for logging, tracking and reporting on Incidents, and the logging, tracking and processing of all Service Requests, related solely to the Managed Applications.
Request Services	Service Desk Services	**13.081**	Provide oversight of Incidents and Service Requests received by the Service Desk that relate to the Managed Applications, including those that need to be escalated by State or third-party resolver groups for final resolution.
Request Services	Service Desk Services	**13.082**	Conduct trend analysis to identify Incident trends, and recommend and implement actions, with State's approval, to reduce Incidents & provide a summary of all workarounds with start, acceptance, and retired dates within the scope of M&O Services provided in this Contract.
Request Services	Service Desk Services	**13.083**	Support the capability for the State to submit, modify and inquire on Incidents within the ITSM system via such media as determined by Contractor and provide reporting from the ticket system.
Request Services	Service Desk Services	**13.084**	Provide the Service Desk Services in English.
Request Services	Service Desk Support	**13.085**	Escalate issues related to the Managed Applications that are not within Contractor's Scope of responsibility.
Request Services	Service Desk Support	**13.086**	In accordance with Contractor's procedures, promptly notify State through the designated communication channel in the event of any Priority Level 1 or Priority Level 2 Incidents.
Request Services	Service Desk Support	**13.087**	The ITSM system shall act as the central repository and single source of truth for ticketing data, information and reporting.
Request Services	Service Desk Support	**13.088**	Contractor shall develop the ability for the State to create and run mutually agreed upon reports from the ITSM System.

Functional Area	Sub Area	Req. #	Requirement
Request Services	Service Desk Support	**13.089**	Contractor shall use the ITSM System of record for Managed Applications for tracking tickets through their lifecycle.
Request Services	Service Desk Support	**13.090**	Provide Level 2 Support and Level 3 Support in accordance with Contractor's responsibilities for the Managed Applications.
Request Services	Service Requests	**13.091**	Contractor shall review and update each Service Request to classify it as a Non-Discretionary Service Request or out of scope. Contractor will estimate the level of effort required to complete each Non-Discretionary Service Request.
Request Services	Service Requests	**13.092**	For any Non-Discretionary Service Request exceeding 250 hours estimated level of effort, Contractor shall notify the State for determination of resolution.
Request Services	Service Requests	**13.093**	Perform technical design activities, including technical solution definition, technical specification and User interface specifications.
Request Services	Service Requests	**13.094**	Participate in design reviews, including the State's business process design review, and design reviews of any Third-Party Vendor.
Request Services	Service Requests	**13.095**	Perform development activities for Minor Releases and Service Requests and coordinate with internal State teams and third-party teams, as necessary.
Reserved		**13.096**	
Request Services	Service Requests	**13.097**	Plan and perform unit and code review for Minor Releases and Service Requests. As necessary, plan and perform functional and integration review for Minor Releases and Service Requests.
Request Services	Service Requests	**13.098**	Correct defects found through testing or reported by State as required by the scope of this Contract.
Request Services	Service Requests	**13.099**	Update technical documentation as appropriate and as required by modifications to the Managed Applications within the scope of this Contract.
Request Services	Service Requests	**13.100**	Comply with the QA procedures and relevant application quality and security standards.

Functional Area	Sub Area	Req. #	Requirement
Request Services	Service Requests	**13.101**	Maintain a Request Fulfillment process (a.k.a. non-discretionary work order process) based upon State's existing process.
Request Services	Service Requests	**13.102**	Provide workflow for submission, tracking, updating, and managing Service Requests.
Request Services	Service Requests	**13.103**	Participate as reasonably requested by State in State's requirements definition and prioritization activities.
Request Services	Service Requests	**13.104**	Coordinate performance tests with Third Party Vendors within a staging environment which replicates the components in the production environment, to the extent possible, to perform the testing functions.
Request Services	Service Requests	**13.105**	Migrate code throughout appropriate environments and incorporate changes into production code baseline.
Security Services	General Requirements	**14.000**	Contractor will adhere to secure application and database configurations and build elements required by the State. Remediation of findings resulting from monthly vulnerability scanning, periodic penetration testing, and Major Release penetration testing activity will be completed within the scope of this Contract.
Security Services	General Requirements	**14.001**	Contractor shall participate in yearly risk assessments used to identify risks to the HSEP platform.
Security Services	General Requirements	**14.002**	Contractor shall participate in Incident response training, tabletop, and testing events as required by Contract.
Security Services	General Requirements	**14.003**	Contractor shall participate in periodic updates to privacy impact assessment documentation.
Security Services	General Requirements	**14.004**	Provide bi-annual entitlement review reports for State attestations and perform remediation of over provisioned or inappropriate access.
Security Services	General Requirements	**14.005**	Contractor will provide federal tax information and Privacy training for all Contractor personnel that handle systems that retain these types of information. Training shall be completed prior to Contractor personnel being granted access to Managed Applications that contain FTI or ACA PII and annually thereafter. Documentation identifying training activities will be made available to audit entities or the State upon request.
Security Services	General Requirements	**14.006**	Responsible for technical code and application configuration remediation activities for ongoing outstanding security weaknesses (identified via audits and POAM findings).

Functional Area	Sub Area	Req. #	Requirement
Security Services	General Requirements	**14.007**	Contractor will maintain current inventory documentation that includes Diagramming and data flows of the Managed Applications and all future development plans.
Security Services	General Requirements	**14.008**	Contractor will assist with maintaining current inventory documentation that includes: Database, Web, Infrastructure and application components.
Security Services	General Requirements	**14.009**	Notify State Security/Privacy Office within 45 minutes of the time Contractor's Privacy Office is made aware of a Security Breach or Notification Event (as defined in Attachment D), identified in the course of day-to-day operational support functions, and enter a corresponding ticket in the Ticket Management system. In addition to the reporting required in Attachment D, for those incidents that are responsibility of Contractor, provide a CMS initial report with minimum information of: • Brief description of the Incident • Incident category (lost stolen, unauthorized access, etc.); • Type of device involved; and • Suspected PII Breach.
Security Services	General Requirements	**14.010**	Upon request, Contractor will provide artifacts for State to maintain and update required security and compliance documents including: • State Security Plan; • Plan of Action and Milestones; and • IRS Corrective Action Plans.
Security Services	General Requirements	**14.011**	Contractor shall perform services, functions and responsibilities identified as its responsibility with respect to the provision, staffing, operation, administration, and management of the Security Services in support of the Managed Applications.
Security Services	General Requirements	**14.012**	The Contractor shall confirm proper security and compliance for Managed Applications as established in Exhibit 3.
Security Services	General Requirements	**14.013**	Comply with applicable Security Policies in Exhibit 3 including CMS policies and the State of Vermont polices, adopted by the State Department of Information and Innovation, the Agency of Human Services Security Policies, and the Vermont Health

Functional Area	Sub Area	Req. #	Requirement
			Connect Policies and procedures, but only if and to the extent such policies and procedures (a) apply to Contractor's scope of work, b) have been provided in writing or a link thereto has been provided to Contractor and (c) if such policies or procedures are updated, revised or changed and the State desires to apply such changes to Contractor, or such changes are required, Contractor shall be provided an opportunity to assess the impact, if any, on its price and schedule obligations, where Contractor's compliance may be subject to the Change Order procedure. State policies are available upon request.
Security Services	General Requirements	**14.014**	Comply with Internal Revenue Service Tax Information Security Guidelines for Federal, State and Local Agencies, Safeguards for Protecting Federal Tax Returns and Return Information (1075).
Security Services	General Requirements	**14.015**	Comply with security measures requested by the State necessary to provide access to any State Facilities.
Security Services	General Requirements	**14.016**	For Notification Events (as defined in Attachment D) that affect the Managed Applications and databases, Contractor shall: • Provide notification of confirmed or unsuccessful Notification Events impacting Contractor-provided or Managed Applications and HSEP databases; • Technical remediation of application configuration or code elements that have identified security flaws as a result of events under the scope of this Contract; and • Report a Notification Event so the State may appropriately inform regulatory agency.
Security Services	General Requirements	**14.017**	Contractor will adhere to secure coding practices and State required secure SDLC process, which entails the following: • Contractor will perform secure code scanning through a service provided by the State; • Remediation of findings with code produced; • Submission of code and secure development scanning leveraging State provided static and dynamic code review tools; • Participate in security impact analysis for all sensitive code promoted to production; and • Documentation of results and dispositions for code remediated.

Functional Area	Sub Area	Req. #	Requirement
Security Services	General Requirements	**14.018**	Contractor agrees to work with State regarding PCI compliance for HSEP payment processing with WEXHealth.
Security Services	General Requirements	**14.019**	Comply with operational guidelines provided by the State to support compliance with NIST 800-53 revision 4.
Security Services	General Requirements	**14.020**	Contractor will operate Contractor's tools within the HSEP that enable monitoring and management capabilities. This excludes administrative access or maintenance for security monitoring tools.
Security Services	General Requirements	**14.021**	Security: • Manage and enforce policies for authentication, encryption, and decryption. • Perform WebCenter user and role management including Federal Cloud access and State internal access. • Install, configure, and support one-way and two-way certificate-based authentication.
Security Services	General Requirements	**14.022**	Contractor shall update the sections of the State Security Plan that relate to the Services covered in this Contract that accurately reflects the HSEP Production Environment as built.
Security Services	General Requirements	**14.023**	Comply with 45 CFR 155.1210.
Security Services	General Requirements	**14.024**	HIPAA Security and Privacy Rules as amended by HITECH, as amended from time to time, and relevant CMS Regulations regarding HIPAA and Information Technology, but only if and to the extent such rules and regulations (a) apply to Contractor's scope of work, (b) Contractor shall be provided an opportunity to assess the impact, if any, of changes to HIPAA on its price and schedule obligations, where Contractor's compliance may be subject to the Change Order procedure.
Service Asset and Configuration Management	General Requirements	**15.000**	Service Asset and Configuration Management processes shall be developed by the Contractor that integrates with State's existing processes and tools (as required). These processes shall be reviewed and approved by State.
Service Asset and	General Requirements	**15.001**	Contractor shall execute applicable activities within the Service Asset and Configuration processes.

Functional Area	Sub Area	Req. #	Requirement
Configuration Management			
Service Asset and Configuration Management	General Requirements	**15.002**	The Contractor shall maintain a Configuration Management Database (CMDB) on behalf of the State which is electronically integrated with Contractor's ITSM System of record that contains Configuration Items, attributes and relationships. The CMDB shall be visible to State at all times.
Service Asset and Configuration Management	General Requirements	**15.003**	Contractor will maintain an Architecture Document to represent the current configuration standards of the HSEP Environments.
Service Asset and Configuration Management	General Requirements	**15.004**	Contractor will assume responsibility for configuring, managing and tracking software at Vermont and non-Vermont locations that are considered part of the Core M&O Services.
Service Asset and Configuration Management	General Requirements	**15.005**	Contractor will coordinate installed software audits with Third Party Vendors as necessary to validate the physical existence of configuration components and accuracy of configuration management data. The Contractor's results of these audits will be reported to State Management team.
Service Asset and Configuration Management	General Requirements	**15.006**	Contractor will maintain and link Change records to CIs and included in scope hardware and software. Such information shall be readily available to view upon request.
Service Asset and Configuration Management	General Requirements	**15.007**	CMDB will be accessible to the Incident, Problem, Change Management and other operational processes; viz. the capability to define many-to-many relationships between process workflow tickets and specific CI's shall be available. Historical information about Incidents, Problems, and Changes for particular CI's shall be readily available.
Service Asset and Configuration Management	General Requirements	**15.008**	Contractor will define the status attributes, e.g. description, status, version, location, etc. for the classes of CIs in scope of the Configuration Management policy.
Service Asset and Configuration Management	General Requirements	**15.009**	Contractor shall provide the State with readable source code and object (executable) code and documentation, in each case solely for functionality developed by Contractor for HSEP.

Functional Area	Sub Area	Req. #	Requirement
Service Asset and Configuration Management	General Requirements	**15.010**	Contractor will control access to the CMDB to clearly defined roles indicating read and edit access.
Service Asset and Configuration Management	General Requirements	**15.011**	Contractor shall provide a standardized mechanism and processes for Conflict Management and data integrity.
Service Asset and Configuration Management	General Requirements	**15.012**	Contractor shall provide version control management capability. Changes to the Managed Applications shall be reported and approved by the State, be maintained in the Contractor's version control management solution, which shall be available to the State for review upon State's request. This version control capability shall be centrally managed by the Contractor and have the capability to deploy all or portions of code, patches, and releases to systems within scope.
Service Asset and Configuration Management	General Requirements	**15.013**	Contractor shall provide a software configuration management solution to store, control, and track instances (baselines during the construction lifecycle) of software configuration items developed for Managed Applications. Such baselines shall be stored in the CMDB and be subject to Change control. Approved production change tickets shall require updates to Configuration Baselines.
Service Asset and Configuration Management	General Requirements	**15.014**	All environments must be kept sufficiently synchronized to confirm testing and release integrity. Evidence of sufficient synchronization must be provided to State through automated configuration management tools.
Service Asset and Configuration Management	General Requirements	**15.015**	With respect to Contractor's responsibilities for the Managed Applications, the Contractor shall have safeguards designed to confirm that the "Last Known good state" of configuration files and variables/parameters/settings are stored and saved for audit, verification and recovery.

Functional Area	Sub Area	Req. #	Requirement
Service Asset and Configuration Management	General Requirements	**15.016**	The Contractor shall deploy logging and monitoring that provides "Drift reporting" for monitoring changes to Configuration Items under management inclusive of applications and configuration files. This Drift report is to track and audit changes that occur outside an approved Changes and existing Request for Change ticket within the Change Management system. The Contractor shall provide drift reports to State upon request and during auditing.
Service Asset and Configuration Management	General Requirements	**15.017**	The Contractor shall maintain an up-to-date relationship/dependency map within the CMDB and make available to State and other HSEP M&O Third Party Vendors upon request.
Service Asset and Configuration Management	General Requirements	**15.018**	Once the data refresh process is defined by Contractor and State and implemented, subsequent data refreshes will occur on a mutually agreed upon basis.
Siebel Asset and Configuration Management	General Requirements	**15.019**	Provide maintenance and support for middleware and supporting utilities, perform middleware system recovery, and perform routine configuration maintenance to support changes in the hosting Environments.
Siebel Services	General Requirements	**16.000**	Maintain Availability, maintainability and monitoring of web, application and database servers.
Siebel Services	General Requirements	**16.001**	Work with Third Party Vendor developers on development/problems that impact Managed Applications
Reserved		**16.002**	
Reserved		**16.003**	
Siebel Services	General Requirements	**16.004**	Perform controlled stops and restarts to middleware servers as needed.
Siebel Services	General Requirements	**16.005**	Monitor, test and apply Siebel patches and hot fixes as needed and as requested by the State at no additional charge: • Unit & System test Siebel Objects; • Conflict resolution (merge vs. over-write) of imported objects; and • Deployment across environments.

Functional Area	Sub Area	Req. #	Requirement
Siebel Services	General Requirements	**16.006**	Provide installation and monitoring of all Siebel middleware and associated components.
Siebel Services	General Requirements	**16.007**	Contractor will perform the following Siebel administrative tasks: • Install/Configure and maintain following server applications: -Gateway; -Siebel server; -Database server; -Web servers; and -BI Publisher. • Configure and maintain the following: -Communication Server SMTP/POP3 -Workflow Monitor Agents -Email Manager Communication templates for workflow; and -Workflow Policies and Actions.
Siebel Services	General Requirements	**16.008**	Maintain the Siebel environments through the performance of the following activities: • Code migration from Development to Production (across all environments). Siebel Remote (as needed). Siebel Anywhere to push out .srf and .rox. Handle issues with Transaction Processor, Merger and Router. Disaster recovery. Support issues with HI States. Support and apply Java upgrades. Siebel High Interactive (HI). Resolve software issues on desktop impacts Siebel HI State. • Maintain/support the organizational access structure for State employees in Siebel: Organizations. Divisions. Positions. Responsibilities. Views. Users/Employees.

Functional Area	Sub Area	Req. #	Requirement
Siebel Services	General Requirements	**16.009**	Support for Siebel Upgrades (Oracle mandate for version compliance) may be subject to Change Request/Change Order and may divert resources from other activities.
Siebel Services	General Requirements	**16.010**	Contractor shall evaluate new patches as they are released by Oracle and other Third-Party Software products being leveraged within the VHC platform and recommend implementation options for State approval. Contractor will provide to State the Enterprise Installation Matrix report once per calendar quarter, at a minimum, and this report shall provide the detail for the current patch levels installed across all HSE environments.
Contractor Personnel	General Requirements	**17.000**	Contractor Personnel will be properly educated, trained and qualified for the HSEP M&O Services they are to perform, and Contractor will put appropriate training in place to meet initial and ongoing training requirements of Contractor Personnel assigned to perform HSEP M&O Services.
Contractor Personnel	General Requirements	**17.001**	All Resources required for the proper performance of HSEP M&O Services by Contractor hereunder shall be under the control, management and supervision of Contractor and Contractor shall be responsible, at its sole cost and expense, for procuring, obtaining and making available, in proper and qualified, professional and high quality working and performing order, all such Resources.
Application Lifecycle Management	ALM Software	**18.001**	Contractor shall provide State access to its Third Party Software ALM tool (“ALM Software”). Contractor shall provide State Third Party Vendor(s) access to its ALM Software, if allowed under ALM Software license.
Application Lifecycle Management	ALM Software	**18.002**	The ALM Software shall support requirements, test case design, test case execution, defect management, requirement traceability matrices, and auditability functionalities.

Functional Area	Sub Area	Req. #	Requirement
Application Lifecycle Management	ALM Software	**18.003**	The ALM Software shall have role-based provisioning including but not limited to read only and roles that can create, edit, and update identified functionalities.
Application Lifecycle Management	ALM Software	**18.004**	The ALM Software shall have the ability to assign defects to an individual and have a custom field to identify company/vendor owner.
Application Lifecycle Management	ALM Software	**18.005**	The ALM Software shall have reportable severity and priority statuses tied to defects that correlate to 1 – Critical, 2 – High, 3 – Medium, and 4 – Low.
Application Lifecycle Management	ALM Software	**18.006**	The ALM Software shall have reportable statuses tied to defects that correlate to new, rejected, open, deferred, assigned, fixed, retest, reopen, and closed.
Application Lifecycle Management	ALM Software	**18.007**	The ALM Software shall have the ability to identify the environment the defect was identified in.
Application Lifecycle Management	ALM Software	**18.008**	The ALM Software shall have the ability to correlate one or more defects to a test case and one or more requirements to a test case.

Functional Area	Sub Area	Req. #	Requirement
Application Lifecycle Management	ALM Software	**18.009**	The ALM Software shall have ability to create test case sets, that are made of one or multiple test case scenarios, each with one or multiple test case steps.
Application Lifecycle Management	ALM Software	**18.010**	The ALM Software shall have the ability to execute created test case sets multiple times and retain statuses of each time it was executed.
Application Lifecycle Management	ALM Software	**18.011**	The ALM Software shall have reportable statuses tied to test cases that correlate to passed, failed, incomplete, roadblocked, and not started statuses.
Application Lifecycle Management	ALM Software	**18.012**	The ALM Software shall have the ability to generate a Requirements Traceability Matrix report for a selected test set provided requirements were linked to the test case(s) in that test set.
Application Lifecycle Management	ALM Software	**18.013**	The ALM Software shall track all changes made by users to identified functionalities and the tracked changes will be able to be viewed by users.
Application Lifecycle Management	ALM Software	**18.014**	In the event the ALM Software is replaced with a different tool, all historical data relating to VHC in the ALM Software shall be exported and provided to the State.

Functional Area	Sub Area	Req. #	Requirement
Application Lifecycle Management	ALM Software	**18.015**	At the end of the Contract, all data relating to VHC in the ALM Software shall be exported and provided to the State.
Application Lifecycle Management	ALM Software	**18.016**	Contractor shall use most current stable enterprise version of the ALM Software.
Application Lifecycle Management	ALM Software	**18.017**	The ALM Software shall be accessible via the product supported internet browser that is mutually agreed to by State and Contractor.
Application Lifecycle Management	ALM Software	**18.018**	The ALM Software shall be supported by vendor manufacturer.
Application Lifecycle Management	ALM Software	**18.019**	The ALM Software shall be able to query and export identified functionalities by users.
Application Lifecycle Management	ALM Software	**18.020**	The ALM Software shall have the ability to customize fields and their values for identified functionalities when mutually agreed to by State and Contractor.

Functional Area	Sub Area	Req. #	Requirement
Application Lifecycle Management	ALM Software	**18.021**	The ALM Software shall have restricted defect status workflows.

EXHIBIT 2
SERVICE LEVEL AGREEMENT

This Exhibit 2 describes the service levels that the Contractor shall meet in performing the M&O Services for the Managed Applications for the State. Any remedy provided in this Exhibit 2 for Contractor's failure to achieve a Service Level, including Service Level credits, shall be the State's sole and exclusive remedy for such failure and shall be further subject to the provisions, limitation and exclusions set forth in Section 8 (Service Level Credit Methodology), Section 8a (At Risk Amount), and Section 8b (Excused Performance) of this Exhibit 2.

This document outlines the Service Level Agreements for the following M&O Services relative to the Managed Applications in the Production Environment and, for some where it is specifically noted, for the Non-Production Environment, where the definitions of such "Environments" is set forth in Section 21 of Attachment A.

Effective from the date of the cutover from the existing environment into the Optum FISMA Environment (OFE) production environment a system stabilization Change Window shall be in effect. The stabilization Change Window shall be in effect for a period of four (4) calendar weeks, after which the OFE migration shall be complete ("Completed OFE Migration"). Provided the OFE migration begins prior to October 1 the stabilization Change Window will not overlap with Open Enrollment. This stabilization Change Window will allow Contractor to focus on stabilizing the application in the new OFE environment. During the stabilization Change Window, Service Level data may be unavailable and SLA reporting may be delayed. Contractor shall continue to monitor all SLA metrics and shall endeavor to report on all Incidents and SLA performance based on the data available.

M&O SLAs and processes will remain in effect during the stabilization Change Window subject to the paragraph above and the exclusions below.

1. All Incidents relating to either the OFE migration or Oracle product upgrades will be excluded from all M&O service level credit calculations, with the exception of the System Incident Notification portion of Service Level #2, during the stabilization Change Window, as defined above.
2. Contractor shall endeavor to meet to the Representative Transaction Performance Measures (Service Level #4) SLA within the Service Metric but will not be subject to service level credit during the stabilization Change Window in accordance with the Change Window exclusion defined in Section 4.2 of this Exhibit.
3. The Plan of Action Milestone (POAM) Remediation and Credits (Service Level #6) may be excused as set forth in Section 6 of this Exhibit for remediation of findings dependent on the OFE migration and/or Oracle product upgrades.

Based on this evaluation, the State may be entitled to an adjustment to the Service Credits for the contracted services.

1 System Availability 83
2 System Incident Notification and Restoration...88

3 Root Cause Analysis/Debrief 91

4 Representative Transaction Performance Measures 91

5 Disaster Recovery (DR) 94

6 Plan of Action and Milestones (POA&M) Remediation Requirements and Credits 94

7 Reconciliation Service Requests 96

8 Service Level Credits Methodology 96

1 System Availability

The System Availability is based on the three (3) Primary Business Components available 24 hours a day, seven days a week for the full calendar month. System Availability is measured for the length of the Contract. The acceptable amount of availability per month is 99.90% for the production environment and 99.50% for specified non-production environments.

1.1 Definitions

Primary Business Component(s) shall be comprised of the following subset of the HSEP Managed Applications: (1) VHC External Portal; (2) VHC Internal Portal; and (3) Siebel

Total Service Minutes - The number of Minutes within the applicable Measurement Period for a Primary Business Component.

Downtime Minutes - The sum of minutes during the applicable Measurement Period that a Primary Business Component under the Contractor's responsibility was not Available for all users or all functions, excluding minutes where the Primary Business Component under the Contractor's responsibility was not Available due to (1) performance of Maintenance during a Maintenance Window; (2) Urgent Service Change; (3) documented problems with the Primary Business Component determined to be not within Contractor's Scope of responsibility under Contractor's Problem Management Process; (4) periods of time attributable to State's failure to approve the installation of Contractor-recommended software patches or upgrades within one week of receipt of a Contractor-initiated Change Request; (5) periods of time attributable to problems, issues, delays or slowness of the Internet or the User's network or equipment; (6) period of time needed to restart the underlying services of the impacted Primary Business Component; or (7) factors that fall within the definition of Excused Performance under Section 8 of this Exhibit 2.

Measurement Period means the applicable full calendar month.

Open Enrollment Period means a period of time defined by CMS and by State of Vermont each year during which Members can enroll in a health insurance plan.

1.2 System Availability Calculation:

For each Primary Business Component during the applicable Measurement Period, Availability is equal to number of Total Service Minutes excluding Downtime Minutes divided by Total Service Minutes during such Measurement Period, with the result expressed as a percentage.

Total Service Minutes = Number of days in the month x 24 hours per day x 60 minutes per hour

Availability % = (Total Service Minutes – Downtime Minutes) / Total Service Minutes x 100

Downtime Minutes:
Total minutes a Primary Business Component is unavailable for all users or all functions during the calendar month

- Maintenance Window minutes that it is unavailable for all users or all functions
- Urgent Service Change minutes that it is unavailable for all users or all functions
- Minutes that it is unavailable for all users or all functions for Items not within Contractor's scope
- Minutes that it is unavailable for all users or all functions when State has not authorized a recommended patch or upgrade
- Minutes that it is unavailable for all users or all functions as a result of the Internet or User network or equipment
- Restart Minutes necessary when it is unavailable for all users or all functions
- Minutes that it is unavailable for all users or all functions for Excused Performance situations

EXAMPLES:

- Example 1

Siebel Primary Business Component in Production is down for 20 minutes on October 7th and 35 minutes on October 20th. During the October 20th outage the server needed to be recycled to restore service. The recycling of the server took 15 minutes. The Availability percentage is computed as follows:

Downtime minutes = 20 + (35 – 15) = 40 minutes
Availability percentage = (44,640 – 40 downtime minutes) / 44,640 x 100 = 99.91%

Conclusion: For the month of October no Service Credit would be assessed for the Availability SLA on the Siebel Primary Business Component.

- Example 2

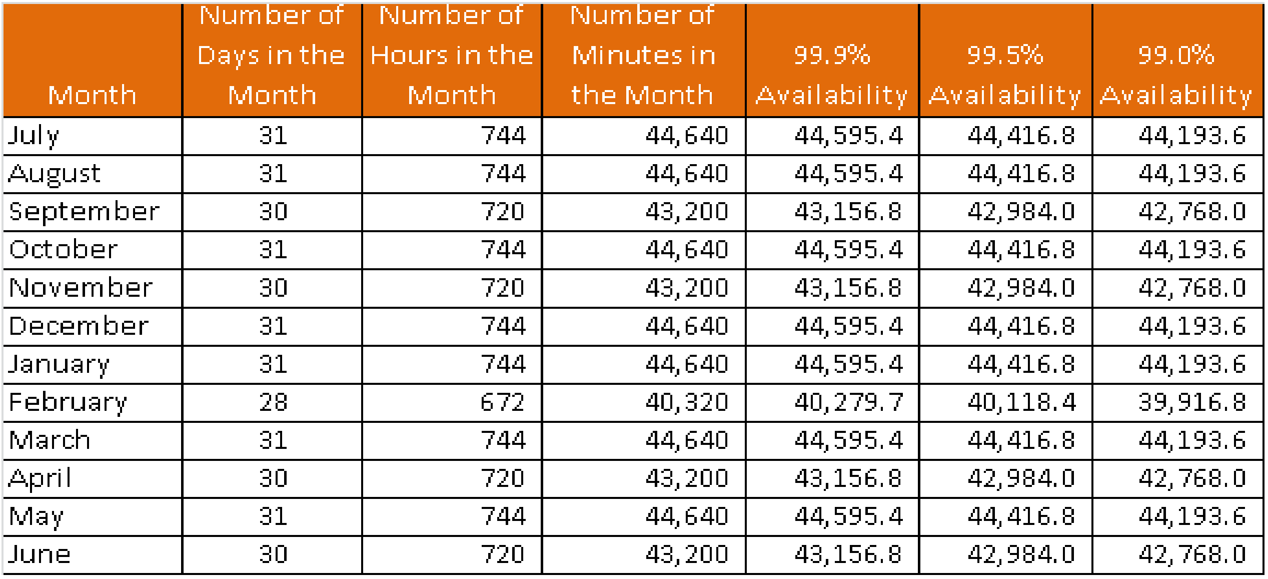
VHC External Portal Primary Business Component in Production is down for 25 minutes on October 7th and 30 minutes on October 20th. The Availability percentage is computed as follows:

Downtime minutes = 25 + 30 = 55 minutes
Availability percentage = (44,640 – 55 downtime minutes) / 44,640 x 100 = 99.87%

Conclusion: For the month of October a Service Credit would be assessed for the Availability SLA on the VHC External Portal Primary Business Component.

Tables A and B provide the Total Service Minutes per month with the computed amounts for specific uptime percentages.

Table A: Total Service Minutes for each Measurement Period and the Computed Availability Percentage Minutes



Month	Number of Days in the Month	Number of Hours in the Month	Number of Minutes in the Month	99.9% Availability	99.5% Availability	99.0% Availability
July	31	744	44,640	44,595.4	44,416.8	44,193.6
August	31	744	44,640	44,595.4	44,416.8	44,193.6
September	30	720	43,200	43,156.8	42,984.0	42,768.0
October	31	744	44,640	44,595.4	44,416.8	44,193.6
November	30	720	43,200	43,156.8	42,984.0	42,768.0
December	31	744	44,640	44,595.4	44,416.8	44,193.6
January	31	744	44,640	44,595.4	44,416.8	44,193.6
February	28	672	40,320	40,279.7	40,118.4	39,916.8
March	31	744	44,640	44,595.4	44,416.8	44,193.6
April	30	720	43,200	43,156.8	42,984.0	42,768.0
May	31	744	44,640	44,595.4	44,416.8	44,193.6
June	30	720	43,200	43,156.8	42,984.0	42,768.0

1.3 Reporting

Contractor shall report System Availability monthly to the State. The report will detail the total amount of Downtime Minutes, the portion the Contractor is responsible for and the percentage of availability. If there are any specific Information Technology Service Management (ITSM) tickets associated with the Downtime Minutes, the identification number and description will be listed on the report.

All times where there are periods of Downtime Minutes where the Contractor was not held liable will be documented in the report with rationale as to why Contractor is excused details and information why.

Contractor shall deliver the report to the AHS IT Manager, DVHA Operations Director, and upload it into the "knowledge repository" no later than the 10th business day of the month following the reporting month. For example, July's report will be due by August 12th. If there is a change of persons for receipt of the report, then the new contact will be provided in a written notice to the Contractor by the State

Service Level Metric for the Managed Application within the Scope of Contractor's responsibility:

Service Level Credit			
	If System Availability is:	Service Level Credit during Open Enrollment equals the following percentage of the HSEP M&O monthly fees as invoiced for the month in which the Service Level default occurred:	Service Level Credit during non-Open Enrollment period equals the following percentage of the HSEP M&O monthly fees as invoiced for the month in which the Service Level default occurred:
Production Environment(s)	Less than 99.90% but greater than or equal to 99.50%	5%	4%
	Less than 99.50% but greater than or equal to 99.00%	8%	7%
	Less than 99.00%	10%	8%
*Non-Production Environments for which Contractor is sole administrator.	Less than 99.50% but greater than or equal to 99.00%	1%	1%
	Less than 99.00% but greater than or equal to 98.00%	2.5%	2.5%
	Less than 98.00%	3%	3%

* The System Availability Service Level shall not be applicable to Non-Production Environments for a period of 90 days after Contract Effective Date. The parties agree that within 4 weeks of the Effective Date, Contactor shall propose the process by which downtime minutes are to be measured.

Earn Back Credits

Parties agree that the desired mutual goal is to have the Primary Business Component Available at or above 99.9% for Production Environments and above 99.5% for Non-production Environments. To this end, State will offer earn back credits when the Contractor is able to maintain consistent Availability at or above 99.9% for Production Environments and above 99.5% for Non-production

Environments for three or more consecutive months in a row. The following sets out the parameters for when the Contractor may receive an earn back credit that can be used to offset any Service Level Credit assessed against Contractor for Managed Application Availability.

If in any month Contractor pays Service Level Credits for any failure to meet the Managed Application Availability Service Level Agreement, as defined above, such Service Level Credits shall establish the maximum "Earn Back Amount" that the Contractor may be entitled to be paid, subject to meeting the following conditions:

1. Contractor must not owe any Service Level Credits for the Managed Application Availability Service SLA for three (3) consecutive months;
2. During such three (3) consecutive month period, the Contractor's actual Managed Application Availability must be within a range set forth in the earn back table below;
3. Contractor shall be entitled to the earn back amount defined in the table below but only beginning on the third (3rd) consecutive month that Contractor's actual Managed Application Availability is within a range set forth in the earn back table below and each successive calendar month thereafter, provided that the Contractor's actual Managed Application Availability in such succeeding calendar month is also within a range set forth in the earn back table below and
4. The amount of the earn back credit beginning in the third and successive calendar months cannot exceed the aggregate amount of Service Level Credits assessed against the Managed Application Availability Service SLA during the Term of this Contract that have not previously been offset by Contractor having earned a subsequent earn back amount.

1.4 Earn Back Credits

	If Availability is:	Earn Back Credit During Open Enrollment. Then the Earn Back Credit equals the following percentage of the monthly fee for Core M&O Services invoiced for the third (3rd) consecutive month in which the Service Level set forth below was achieved and for each successive calendar month thereafter, subject to the conditions noted above:	Earn Back Credit During non-Open Enrollment period. Then the Earn Back Credit equals the following percentage of the monthly fee for Core M&O Services invoiced for the third (3rd) successive month in which the Service Level set forth below was achieved and for each successive calendar month thereafter, subject to the conditions noted above:

Production environments	Less than 100.0% but not less than 99.95%	5%	4%
	Less than 99.95% but not less than 99.90%	4%	3%
Non-Production environments	Less than 99.90% but not less than 99.80%	2%	2%
	Less than 99.80% but not less than 99.50%	1%	1 %

If Contractor's actual Primary Business Component Availability for the third successive calendar month or for any calendar month thereafter fails to be at a level corresponding to an earn back credit, then no earn back credit shall be owed until Contractor's actual Primary Business Component Availability is at a level corresponding to an earn back credit for three (3) consecutive months.

Example:

- Per Example 2 above in Section 1.2, Availability was 99.87%, which resulted in a Service Level Credit of 5% being issued in connection with the October invoice.
- In November, December and January, no Service Level Credits for Availability were assessed for any Primary Business Components. Downtime totaled 10, 20 and 15 minutes, respectively, which means availability was computed as follows:

  November Availability percentage = (43,200 – 10 downtime minutes) / 43,200 x 100 = 99.98%
  December Availability percentage = (44,640 – 20 downtime minutes) / 44,640 x 100 = 99.96%
  January Availability percentage = (44,640 – 15 downtime minutes) / 44,640 x 100 = 99.97%

- Availability during the 3-month period from November through January was less than 100.00% but not less than 99.95%, which results in an Earn Back Credit being issued in connection with the January invoice of 5%.

Upon termination or expiration of the Contract, any unliquidated Earn Back Credits shall expire.

2 System Incident Notification and Restoration

The system incident notification and restoration SLA is a report of all Priority Level 1and Priority Level 2 incidents that occurred during the month with their response, notification, and resolution times. The Contractor opens all Priority Level 1 and Priority Level 2 tickets and SLA measurements shall be taken from the Contractor generated tickets.

2.1 Notification Calculation - When the Contractor is made aware of a system issue from an email, phone call to on-call manager, probe failure, or event monitoring alert, the Contractor shall create and or respond to the ticket with escalated priority and perform a system health check to determine if the incident qualifies as either Priority Level 1 or Priority Level 2.

Once an incident has been established as either Priority Level 1 or Priority Level 2, an internal war room page out shall be sent to the Contractor's triage team by the Contractor's Technology Command Center (TCC). Start time shall be taken from the timestamp within the ticketing system of the first member of the Contractor's triage team receiving the page out ("Initial Notification Start Time"). Contractor shall notify the State within fifteen (15) minutes for Priority 1 and within one (1) hour for Priority 2 ("Initial Notification"). Status updates shall be delivered hourly until the incident is resolved. If an incident is not resolved during the first twenty-four (24) hours, then one status report shall be delivered at the end of each business day until it is resolved.

There are certain cases when a Contractor enterprise wide P1 or P2 has already started, and later impacts VHC Managed Applications. In these cases, Initial Notification Start Time will be calculated from the page out time after a VHC service has been triaged and confirmed to be impacted as part of the enterprise wide P1 or P2 by the TCC. Initial Notifications shall be manually generated and sent to the State by the Contractor in these instances outside of the ITSM tool.

2.2 Restoration calculation – Restoration metric is calculated as the number of Incidents for Priority 1 and Priority 2 Incidents that are restored outside the agreed upon time for each priority during the applicable measurement period.

Start time will be taken from the timestamp within the ticketing system of the first member of the Contractor's triage team joining the war room ("Restoration Start Time"). If a P2 is upgraded to a P1, the start time starts at the time of the upgrade, understanding the Service Level Metric will be for a P1. All P1 and P2 incidents and their start and end times will be reviewed and mutually agreed upon by both parties in a review meeting within two (2) weeks of the occurrence.

There are certain cases when a Contractor enterprise wide P1 or P2 has already started, and later impacts VHC Managed Applications. In these cases, the Restoration Start Time will be calculated from the time the Contractor joins the war room after a VHC service has been triaged and confirmed to be impacted as part of the enterprise wide P1 or P2 by the TCC.

System incident restoration is measured for the length of the Contract. Restoration time for incidents will be under four (4) hours for Priority 1 incidents, under eight (8) hours for Priority 2 incidents.

2.3 Definitions

Table C provides when Priority level 1 and Priority level 2 incidents resolution work starts and completes, how often status notifications are sent, and how they are measured. The column header names for this table mean the following:

Priority Level: The priority classification level.
Restoration: The Incident is considered "restored" when impact has been removed by implementing a work around or by implementing a solution and that Contractor submits to

the State for its agreement that the impact has been removed. The Service Level for the Incident is met if either a work around or a solution is implemented prior to the corresponding restoration Service Level Metric. Once a work around or solution has been identified, or a subsequent change has been identified, the actual work needs to be implemented via the agreed upon change management process.
Restoration Start Time: The time the Contractor has joined the Incident war room and shall start working on a resolution for that incident. The Contractor shall join the Incident war room within the amount of time identified in Table C below after the Contractor has received the internal page out for an Incident war room after an incident has been established as either Priority Level 1 or Priority Level 2.
Restoration Time: The maximum amount of time from the Restoration Start Time until the Incident has a Restoration.
Initial Notification Start Time: The time at which the Contractor's triage team has received the internal page out for an Incident war room after an incident has been established as either Priority Level 1 or Priority Level 2.
Initial Notification: The maximum amount of time from the Initial Notification Start Time until when the initial notification must be sent.
Status Update Notifications: The frequency of when status notifications must be sent during the first 24 hours from when an issue is established as an incident until incident resolution.
Post 24-hour Status Update Notifications: The frequency of when status notifications must be sent after the initial 24 hours (unless mutually agreed) from when an issue is established as an incident until incident resolution.
Measurement Tracking: How the notification and resolution times are measured and reported.

Table C: Incident Notification and Restoration Times

Priority Level	Restoration Start Time	Restoration Time	Initial Notification	Status Update Notifications	Post 24-hour Status Update Notifications	Measurement Tracking
Level 1 Incidents (P1)	Within 15 minutes	Within 4 hours	Within 15 minutes	Every 1 hours	Daily at the end of each business day	Reported monthly in System Availability reports.
Level 2 Incidents (P2)	Within one hour	Within 8 hours	Within 60 minutes	Every 1 hours	Daily at the end of each business day	Reported monthly in System Availability reports.

2.4 Reporting

Contractor shall report System Incident Notification and Restoration monthly to the State. The report will detail all incidents for the month by ITSM identification number, description, priority level, open date time, closed date time, and the date time each notification was sent. All times shall be reported in Eastern Time.

Contractor shall deliver the report to the AHS IT Manager, DVHA Operations Director, and upload it into the "knowledge repository" no later than the 10th business day of the month following the reporting month. If there is a change of persons for receipt of the report, then the new contact will be provided in a written notice to the Contractor by the State. For example, July's report will be due by August 12th.

Certain ITSM fields are not visible to the State due for VHC incidents based on incident type and provisioning. Contractor shall screenshare or provide screenshots with the fields used for SLA calculations.

Service Level Credit	0.25% reduction of the monthly fee for Core M&O Services invoiced for the month in which a Service Level default occurred for each P1/P2 for which the incident notifications identified in table C where not met, with a maximum of up to the At-Risk Amount. 0.5% reduction of the monthly fee for Core M&O services invoiced for the month in which a Service Level default occurred for each P1/P2 incident for which the restoration times identified in table C where not met, with a maximum of up to the At-Risk amount

2.5 Out of Scope

Security Incidents that do not impact system availability are not subject to this Service Level or Service Level credits, notwithstanding whether they are characterized as Priority Level 1 or 2 Incidents unless the Security Breach resulted solely from Contractor's failure to maintain appropriate security measures to prevent such Security Incidents.

This Restoration Time Service Level shall exclude Excused Performance, as defined under Service Level Credits herein.

For Incidents unrelated to scope of Contractor's responsibility or caused by systems or third parties outside the scope of Contractor's responsibility, the information within the notification will depend on the information available to the Contractor.

3 Root Cause Analysis/Debrief

Root Cause analysis will provide details to the origin of P1 and P2 incidents. The Root Cause Analysis documentation shall, to the extent Contractor is able to make such determinations, include what happened, why it happened, and identify what changes need to be made to prevent it from happening again. Contractor shall follow the CMS Guidance for Performing Root Cause Analysis with Performance Improvement Projects documentation which can be found at: https://www.cms.gov/medicare/provider-enrollment-and-certification/qapi/downloads/guidanceforrca.pdf .

The Root Cause Debrief and Root Cause Analysis document will clearly include:

- A detailed description of the incident; and
- A probable root cause of the incident.

Root Cause Analysis (RCA) status (validated, still under investigation, fixed) will clearly include:

- Identify the team working on the permanent fix;

- A description of next steps to be taken (including the code changes that need to be made); and
- A timeline for the implementation of the fix.

3.1 Reporting

Contractor shall deliver a written Root Cause Debrief to the AHS IT Manager, DVHA Operations Director, and uploaded to the "knowledge repository" within four (4) business days of the incident closure. Contractor will present to the State the Root Cause Debrief and answer follow up questions that the State may request for clarifications or further detail.

Contractor shall deliver a written Root Cause Analysis to the AHS IT Manager, DVHA Operations Director, and uploaded to the "knowledge repository" within twenty (20) business days for the final RCA delivery from the time of the incident closure for the Contractor's areas of responsibility under this Contract.

Should the Root Cause Analysis documentation include a recommendation that change(s) to the system or processes should be implemented to reduce the likelihood of a future similar incident, Contractor shall work with the State to determine the appropriate course of action. In the event a change is outside of the Contractor's responsibility the State will work with the appropriate Third-Party Vendor to determine the appropriate course of action.

Service Level Credit	0.5% reduction of the monthly fee for Core M&O Services invoiced for the month in which a P1/P2 Root Cause Debrief was delivered late, with a maximum of up to the At-Risk Amount.

4 Representative Transaction Performance Measures

Representative transaction performance measures are based on all high usage transaction response time. Transaction performance is measured for the length of the Contract. The average transaction performance level for production environments is two (2) seconds. Below is the list of transactions that will be monitored:

- Login
- Responsibility Page
- Privacy Page
- Voter Registration Page
- Restart Application
- Log out

4.1 Reporting

Contractor shall report System Transaction Performance monthly. The report shall show highest, lowest and average length of time for each of the listed transactions with the total number of each transaction by day, week, and month.

Contractor shall deliver the report to the AHS IT Manager, DVHA Operations Director, and upload it into the "knowledge repository" no later than the 10th business day of the month following the reporting month. If there is a change of persons for receipt of the report, then the new contact will be provided in a written notice to the Contractor by the State. For example, July's report will be due by August 12th.

4.2 Definitions

Transactions: The agreed internal and external production transactions executed by Contractor tools in Managed Application(s). Requests that are User functions or other functions outside the Contractor scope of responsibility will not be considered as Transactions.

Contractor Application Services Domain: This is Contractor's internal portion of the production Managed Application platform(s), which is within the Contractor's scope of responsibility. It excludes various user interactions, network firewalls, or other security boundary devices outside of the Contractor's scope of responsibilities.

Elapsed Duration or Operation Time: Elapsed duration or Operation Time for a Transaction is the time between the receipt of the Transaction request at the point of entry (web server or other device) to the Contractor Application Services Domain and the time the Transaction reply exits the Contractor Application Services Domain at the point of exit (web server or other device).

Notwithstanding the foregoing, for any Transaction that commenced during one of the following periods, Elapsed Duration shall not commence until the following periods have ended:

(1) Periods of time when Maintenance is being performed during a Maintenance Window;

(2) Periods of time when a Change is being performed during a Change Window;

(3) Periods of time when documented problems with Managed Applications exist that are not within Contractor's Scope of responsibility (e.g., State-managed DNS, networks, interfaces to third parties, etc.), to the extent that such problems cause the Transaction to be delayed; and

(4) Periods of time when a Transaction cannot be completed as a result of the State's failure to approve the installation of Contractor-recommended software patches or upgrades.

Measurement Period: HSEP/VHC Business Hours of Operations during the applicable full calendar month.

Calculation: The average Transaction load time during the applicable Measurement Period.

Performance: Steady State	
Type	Service Level
Measurement Period	HSEP Business Hours of Operations during the applicable full calendar month.
Description	This Service Level measures the percentage of certain production Transactions executed solely within the Contractor's scope of responsibility domain that are completed within the required timeframe.

Reporting Period	Monthly
Service Metric	Average Operation Time per day within the HSEP/VHC Business Hours of Operation for the identified transactions is within **2.0 seconds**

Service Level Credit		
If avg. transaction time is:	Service Level Credit during Open Enrollment. Then the Service Level credit equals the following percentage of the monthly fee for HSEP Maintenance and Operations invoiced for the month in which the Service Level default occurred:	Service Level Credit during non-Open Enrollment period. Then the Service Level credit equals the following percentage of the monthly fee for HSEP Maintenance and Operations invoiced for the month in which the Service Level default occurred:
Greater than 2.0 seconds but less than or equal to 2.5 seconds	1%	0.50%
Greater than 2.5 seconds but less than or equal to 2.75 seconds	1.50%	0.70%
Greater than 2.75 seconds but less than or equal to 3.0 seconds	2.00%	0.90%
Greater than 3.0 seconds	2.50%	1.00%

There are no Service Level Credits for non-production environments.

5 Disaster Recovery (DR)

In the event of a disaster the Contractor shall meet the following services levels when restoring HSEP Managed Applications as delineated in Attachment A, Section 6.1.1, Table 1.

Disaster Recovery RTO and RPO Service Level Agreement and Credits	
Type	Service Level
Commencement	TBD
Description	In the event of a Disaster, Contractor will meet the RPO and RTO to recover, as specified in the DRP, the Production and Support Environments, to the DR environment.
Reporting Period	Per Incident.

Calculation	The Service Level will be measured from the time a Disaster is declared (pursuant to agreed procedures) and Availability has been restored to the affected non-DR Environments. The Production Applications must be accessible to the State's remote application administrators and Users to begin the verification process.
Data Sources	N/A
Service Level Metric Production and Supporting Environment(s)	Recovery Time Objective = 8 Hours Recovery Point Objective = 30 Minutes
Service Level Metric for all other, non- DR Environments	Recovery Time Objective = 48 Hours Recovery Point Objective = 24 Hours
Service Level Credit	If either the RPO or RTO requirements are not met, the Service Level Credit will be 10% reduction of the fixed monthly fee for Core M&O Services invoiced for the month in which the Service Level default occurred, with a maximum up to At-Risk Amount.

6 Plan of Action and Milestones (POA&M) Remediation Requirements and Credits

The POA&M is a remedial action plan which documents weaknesses, risk rankings, and planned progress milestones towards remediation activities. Contractor shall follow CMS guidance for POA&M documentation, which can be found at:

https://www.cms.gov/Research-Statistics-Data-and-Systems/CMS-Information-Technology/InformationSecurity/Downloads/RMH_VIII_6-2_Plan_of_Action_and_Milestones_Process_Guide.pdf

Contractor shall complete the exercise in Table 1 for every newly identified POA&M item during the term of the Contract within Contractor's responsibility. Table 1 provides the Service Level requirements for POA&M items. Contractor's obligations with respect to remediating any existing or future POA&M findings, where such remediation requires upgrading or migrating the State's Oracle software into Contractor's OFE in order to complete the remediation, will be waived until the Completed OFE Migration, at which point Contractor's obligations resume. To the extent OFE migration is delayed due to State decision, any POA&M findings requiring remediation in OFE will be Excused Performance and no Service Level Credit will be applied.

Commencement Phase: The first date in which parties begin to meet post Identification. Commencement Phase ends upon Contractor acceptance of responsibility, weakness is validated, risk determined to calculate expected completion date, preliminary milestones, dates, and resources are provided, at which point Remediation Status begins.

Controls: The MARS-E Version 2.0 security controls are in scope for assessments under this Service Level.

Data Sources: Possible origins of POA&M items.

Identification Date: The date when a weakness is identified by either party, but it is not yet determined to be Contractor's Responsibility.

Remediation Status: The time period from end of Commencement Phase to Remediation Date, which is the period of time used to measure the Service Level Metric.

Remediation Date: The date upon which a POA&M item is sent by Contractor to the State in a pending closed status. POA&M item is still subject to State and CMS review/approval, but the Service Level Metric would pause once a pending closed status is sent by Contractor. Should State/CMS reject the remediation plan, Contractor would have an additional thirty (30) days from date of notice of rejection to perform additional remediation activities prior to the Service Level Metric starting again.

Service Level Metric for POA&M Entries: The amount of time measured between end of Commencement Phase and Remediation Date of a POA&M item based on the risk type.

Table 1 – POA&M Service Level Requirements

Service Level			
Identification and Commencement Phase	**Remediation Status**	**Data Sources**	**Service Level Metric**
Upon the Identification Date of a weakness against Controls, Contractor and State will initiate the Commencement phase. Initiate Commencement Phase - the following 3 steps must occur within 30 calendar days unless excused performance or otherwise agreed to by the parties: (1) State and Contractor meet to validate identified weakness and determine ownership; (2) Contractor will draft and submit plans of action milestones, target completion dates for each milestone, and resources required; and (3) The State will confirm acceptance of contractor POA&M data submission(s), providing risk ranking changes (if	Period of time that begins upon completion of Commencement Phase, where Contractor will engage in Remediation activities, updating State throughout the process. State will update the POA&M as appropriate until Remediation Date.	Data sources used in assessments against the Controls include the following: • independent assessments • self-attestations • vulnerability assessments • pen test or • incident/risk reports	Contractor shall Remediate the severity of risk as follows unless as otherwise agreed to by both parties: High ranked risks – shall not exceed more than 90 days in Remediation Status (period of time from the end of the Commencement Phase to Remediation Date). Moderate ranked risks – shall not exceed more than 180 days in Remediation Status (period of time from the end of the Commencement Phase to Remediation Date). Low ranked risks – shall not exceed more than 365 days in Remediation Status (period of time from the end of the Commencement Phase to Remediation Date).

necessary) and initiate entry to State POA&M;			

Service Level	
Service Level Credit	0.25% reduction of the monthly fee for Core M&O Services invoiced for the month in which a Service Level default occurred for each POA&M that did not meet the Service Level Metric in Table 1, with a maximum of up to a 3% reduction of the Core M&O Services invoice per month.

7 Reconciliation Service Requests – 834 Transaction Removal

Reconciliation Services shall be performed according to Section 6.2.2 of Attachment A.

8 Service Level Credits Methodology

This section describes the methodology for calculating service level credits which will be awarded to the State by the Contractor in the event the Contractor fails to meet the agreed upon service level goals mentioned above.

Service Level Credits: Contractor's monthly Service Level report shall include information on any Service Level default(s) and corresponding Service Level credit(s). Contractor shall automatically provide service level credits. If Contractor fails to do so, within 90 days of State's receipt of the applicable Service Level report, State may elect to claim a Service Level credit by issuing a written notice to Contractor. If more than one Service Level default has occurred within a single month, the sum of the corresponding Service Level credits (up to the At-Risk Amount) may be claimed by State.

If a single Incident results in multiple Service Level defaults, as determined through Contractor's root cause analysis, State shall be entitled to claim a maximum of 5% of the fixed monthly fee for HSEP Maintenance and Operations per calendar month for that Incident, unless the single Incident is either specific to Availability or Disaster Recovery, and such failure individually results in a Service Level Credit greater than the five percent (5%) of the monthly fixed monthly fee for HSEP Maintenance and Operations fee. Except as set forth below, the State may not elect to seek actual damages related to the same events for which Service Level credits were assessed as the Service Level Credits are the State's sole and exclusive remedy.

Service credits credited here under shall not be deemed a penalty, but rather a cost adjustment attributable to the lower level of service delivery. Contractor acknowledges and agrees that Services delivered hereunder which do not meet the Service Levels set forth herein have inherently less value for the State and the Service Level Credits represent a fair value for the services actually delivered; provided, however, the State shall retain all of its remedies in law or at equity in the event the Production Environment is unavailable eight (8) or more hours per week (as defined in this exhibit, under SLA 1 System Availability), in any given month, subject to the Contractor's actual limitation on damages as set forth in this Contract, Attachment D.

a) At-Risk Amount: The At-Risk Amount is the maximum amount of Service Level credits under this Contract that the State may receive in the aggregate for Service Level defaults occurring during a single calendar month unless otherwise specified above in the various SLA metrics. The "At-Risk Amount" shall be ten percent (10%) of the monthly fee for Core M&O Services, as determined in accordance with Attachment B, Payment Provisions, that are payable by State to Contractor during the calendar month in which the Service Level default(s) occurred. Service Level Credits associated with System Availability will be assessed first for purposes related to the Earn Back process for System Availability.

b) Excused Performance.
To the extent that any Service Level default is solely attributable to the following, then in any case, the corresponding Service Level default shall be excused, either entirely or partially. To the extent that any Service Level default is partially attributable to the following, then in any case, the proportion at which was partially attributable to the corresponding Service Level default shall be excused with respect to that Service Level:

(A) Anything outside the scope of Contractor's responsibility for Managed Applications as defined in Section 6, Table 1 for Attachment A is excluded from any Service Level;

(B) A State Delay in responding to a request for approval;

(C) A Force Majeure Event; except that a Force Majeure Event shall not excuse, delay or suspend Contractor's obligation to invoke and follow its Business Continuity Plan, Disaster Recovery Plan or any other business continuity or disaster recovery obligations set forth in this Contract in a timely fashion;

(D) A default by State, a Third-Party Vendor of State or any other third party (excluding Third Party Vendors provided by Contractor or other third parties engaged by Contractor in relation to the Services) which directly prevents Contractor from meeting the applicable Service Level;

(E) External Systems;

(F) A CMS policy change which directly impedes Contractor's ability to perform the Services hereunder;

(G) Acts or omissions of State, a State Third Party Vendor or other third party (excluding Third Party Vendors provided by Contractor or other third parties engaged by Contractor in relation to these or any other services provided under an agreement with the State); or

(H) The failure of the State or a State Third Party Vendor other than the Contractor related to their performance of any disaster recovery obligations in a timely fashion including where that Third-Party Vendor is the Contractor under a separate hosting services contract.

EXHIBIT 3
SECURITY POLICIES

Contractor and its permitted assignees and subcontractors shall comply with information/technology control policies and standards applicable to the security of data for the Services provided under this Contract as listed below:

1. Compliance with version 2.0 of CMS' Minimum Acceptable Risk Standards for Health Insurance Exchanges.

2. State of Vermont Security Policies, adopted by the State Agency of Digital Services, the Agency of Human Services Security Policies, and the Vermont Health Connect Policies and procedures, but only if and to the extent such policies and procedures: (a) apply to Contractor's scope of work; b) have been provided in writing or a link thereto has been provided to Contractor; and (c) if such policies or procedures are changed by the State and the State desires to apply such changes to Contractor, Contractor shall be provided an opportunity to assess the impact, if any, on its price and schedule obligations, where Contractor's compliance may be subject to the Change Order procedure set forth in this Contract. These policies are available upon request.

3. Compliance with 45 CFR 155.1210.

4. Internal Revenue Service Tax Information Security Guidelines for Federal, State and Local Agencies, Safeguards for Protecting Federal Tax Returns and Return Information (IRS Publication 1075).

5. HIPAA Security and Privacy Rules as amended by HITECH, as amended from time to time, and relevant CMS Regulations regarding HIPAA and Information Technology, but only if and to the extent such rules and regulations: (a) apply to Contractor's scope of work and (b) Contractor shall be provided an opportunity to assess the impact, if any, on its price and schedule obligations, where Contractor's compliance may be subject to the Change Order procedure set forth in this Contract.

6. Prior to placement of Contractor Personnel on the project, the State will provide the appropriate level of privacy and security compliance training to Contractor Personnel as deemed necessary by the State at State's sole cost and expense.

7. Security measures requested by the State necessary to provide access to any State Facilities.

8. Contractor agrees to participate in IRS Publication 1075 and MARS-E Version 2.0 assessments (such as self-attestations) to help ensure the necessary controls are in place and provide the necessary security deliverables related to these assessments but only if and to the extent such rules and regulations: (a) apply to Contractor's scope of work; and (b) when assessment/audit events are identified outside the anticipated Audits as described below, Contractor shall be provided an opportunity to assess the impact, if any, on its price and schedule obligations, where Contractor's compliance may be subject to the Change Order procedure set forth in this Contract.

Anticipated Audits during each year of the contract term or as otherwise listed below:

- Independent Assessment Audit of the 3 sites containing live data for the Authority to Connect (ATC), as needed on a date to be determined by the parties in approximately Q2 2023.
- Independent Assessment, in lieu of self-Attestation due on a date to be determined by the parties in approximately the second calendar quarter annually.
- IRS Safeguards audit of the 3 sites containing FTI data on a date to be determined by the IRS in 2021 or 2022.

EXHIBIT 4
DELIVERABLE BEST PRACTICES

Deliverables shall be in English and will utilize the Contractor's style guide. Deliverables will be written for the intended audience; user manuals should be written for business users and design documents should be written for technical staff. There should be no embedded documents. With the exception of security documents, links to related material should point to documents on the State SharePoint. Deliverables are to be approved based on the Acceptance criteria agreed to in the associated Deliverable Expectation Document (DED). Deliverable Acceptance is subject to the schedule outlined in Attachment A, Deliverable Review and Approval Process, Section 15.

Those artifacts, or sections thereof, provided in conjunction with Deliverables to meet M&O DED criteria will be reviewed as part of the Deliverable Review and Approval Process. Review will take place during the next iteration of the Deliverable in which it is used.

Supplemental material, including third party documents and/or documents created under different contracts, may be provided to direct readers to related information that is not part of the DED criteria in the Deliverable. This supplemental material will not be reviewed as part of the Deliverable Review and Approval Process.

Deliverables must include the following components.

- Cover Sheet;
- Revision History – record of changes and who made the changes;
- Table of Content – list of major sections in the document (include table of figures if applicable);
- Objective – the purpose of the document; and
- Scope – content as defined by the DED.

Deliverables will not be submitted without first being proofread by the Contractor to help ensure all spelling and grammar errors are fixed. Contractor Deliverables are to be complete and in a final draft before requesting review from the State.

Deliverables will be maintained throughout the life of this agreement. If a Change Request or defect causes a modification to the system, any Deliverable pertaining to that functionality will be reviewed and updated appropriately. Updates will be made as set forth in this Contract to meet DED criteria during the next scheduled Deliverable iteration.

EXHIBIT 5

STANDARD FORM TEMPLATE QUALITY ASSURANCE SURVEILLANCE PLAN (QASP)

Quality Assurance Surveillance Plan

INTRODUCTION

This Quality Assurance Surveillance Plan (QASP) has been developed to evaluate Contractor actions while implementing the Statement of Objectives. It is designed to provide an effective method of monitoring Contractor performance for each listed objective on the Performance Requirements Matrix. It also provides a systematic method to evaluate the services the Contractor is required to furnish.

STANDARD

The Contractor is responsible for management and quality control actions to meet the terms of the contract. The role of the Product Owner (PO) and Vermont Product Team is quality assurance to ensure contract standards are achieved.

The Contractor shall perform all work required in a satisfactory manner in accordance with the requirements of the contract. The Contractor shall notify the Product Owner for appropriate action if it is likely that the Contractor will not achieve successful final delivery of the software code in accordance with the performance objectives and acceptable quality levels (AQLs) identified below.

PERFORMANCE REQUIREMENTS MATRIX

The Vermont Product Team will evaluate the performance objectives reflected below by reviews and acceptance of work products and services. As indicated, the Vermont Product Team will assess progress towards the final delivered software code. Note that the performance requirements listed below are required for the final deliverables. However, the sprints and incremental delivery of code will be assessed by the Vermont Product Team to ensure that the Contractor is on a path to successful final delivery.

Contractor **Deliverable**	**Contractor Performance Standards(s)**	**Contractor Acceptable Quality Level**	**State** **Method of Assessment**
Tested Code	Code delivered under the contract must have substantial test code coverage and a clean code base. Version-controlled Vermont GitHub repository of code that	Minimum of 90% test coverage of all code	Combination of manual review and automated testing

Contractor **Deliverable**	**Contractor Performance Standards(s)**	**Contractor Acceptable Quality Level**	**State** **Method of Assessment**
	comprises product that will remain in the public domain.		
Properly Styled Code	GSA 18F Front End Guide	0 linting errors and 0 warnings	Combination of manual review and automated testing
Accessible	Web Content Accessibility Guidelines 2.1 AA (WCAG 2.1 AA) standards	0 errors reported for WCAG 2.1 AA standards using an automated scanner and 0 errors reported in manual testing	https://github.com/pa11y/pa11y
Deployed	Code must successfully build and deploy into staging environment and must be compatible with data schemas used in production. If data schemas are not available, code must successfully build and deploy into production environment.	Successful build with a single command.	Combination of manual review and automated testing.
Documentation	All dependencies are listed, and the licenses are documented. Major functionality in the software/source code is documented.	Individual methods are documented inline using comments that permit the use of tools such as JsDoc. System diagram is provided.	Combination of manual review and automated testing, if available.
Secure	OWASP Application Security Verification Standard 3.0 and meet the requirements of an application in a CMS MARS-E compliant environment.	Code submitted must be free of medium- and high-level static and dynamic security vulnerabilities.	Clean tests from a static testing SaaS (such as Veracode or Snyk) and from OWASP ZAP, along with documentation explaining any false positives

Contractor **Deliverable**	**Contractor Performance Standards(s)**	**Contractor Acceptable Quality Level**	**State** **Method of Assessment**
User Research and Design Artifacts	Design research and usability testing activities must be conducted at regular intervals throughout the development process (not just at the beginning or end) to ensure the user needs are well understood and that design solutions work well for users.	During the first sprint, vendor shall establish a design research plan in collaboration with the Product Team. This plan must account for the availability of resources, articulation of research methods, and delivery of research-related records. In subsequent sprints, research-related records will be delivered in accordance with the design research plan.	Cross-reference research-related records with other project documentation to ensure that research is properly accounted for and communicated.

PROCEDURES

Delivery of all software assets will occur by pull request from the Contractor's repository to the appropriate Vermont repository. If inspection results are satisfactory, the pull request will be merged; otherwise, deficiencies will be noted in the pull request or through issues as described below. The Vermont Product Team and PO may find the delivery satisfactory even though further work is required in the next sprint.

At the conclusion of each sprint, the Vermont Product Team will review the related functionality to ensure compliance with acceptance criteria and requirements of the user stories. All clarifications and changes to the user stories during the sprint that are agreed upon are documented in the issue tracker. Incomplete or inadequate code and user stories will be noted in a mutually agreed-upon issue tracker with links to each issue shared with the PO. The Contractor may respond in that tracker as appropriate, addressing the accuracy and validity of the defect as well as any planned corrective action (if not already noted). The issue tracker will be updated as revised acceptance criteria are added to the incomplete backlog items as part of the backlog grooming process. The Contractor's team will discuss and document actions to prevent recurrence in the sprint retrospectives.

At the conclusion of the period of performance, the Vermont Product Team will follow a similar procedure to document discrepancies and to assess overall performance.

ACCEPTANCE OF SERVICES

The Product Owner shall review all work products for compliance with performance standards described in the SOO and monitoring procedures described in this QASP. The PO shall not accept work products for the contract until all defects have been corrected.

EXHIBIT 6

INFORMATIONAL MEMORANDUM

TO: State of Vermont, Department of Vermont Health Access
Authorized Representative

FROM: Scott Cerreta, OptumInsight, Inc.

SUBJECT: Discretionary Funds Informational Memorandum Between State of Vermont
and Contractor OptumInsight, Inc.
Contract Number 31750

In accordance with Attachment B, Section 9.2, Amendment 2 to the OptumInsight, Inc. (Optum) contract #31750, parties acknowledge that Discretionary Services completed within a given State Fiscal Year (SFY) shall be funded by the Discretionary Services budget allocated for that SFY regardless of when the work began. Work started, but not completed within a specific SFY shall be noted by Contractor in this Informational Memorandum and acknowledged by the State Authorized Representative no later than May 15th of the current SFY. Work that starts in the current SFY and is completed in the next SFY shall be invoiced by Contractor and paid in full by State in accordance with the terms of the Change Request. The following information shall be provided:

Change Request Number:	Work Start Date:	Anticipated Work End Date:	Description of work:	Reason for delay and/or carry forward:	Estimated value of work to be completed in next SFY:

Submitted by:

Date of Submission:

Signature: ____

State Acknowledgement of Receipt

Acknowledged by: ____
State Authorized Representative

Date of Acknowledgement: ____

Exhibit 7: Quality Assurance Surveillance Plan (QASP) for Section 26 Premium Processing Development

INTRODUCTION

This Quality Assurance Surveillance Plan (QASP) has been developed to evaluate Contractor actions while implementing the Statement of Objectives. It is designed to provide an effective method of monitoring Contractor performance for each listed objective on the Performance Requirements Matrix. It also provides a systematic method to evaluate the services the Contractor is required to furnish.

STANDARD

The Contractor is responsible for management and quality control actions to meet the terms of the contract. The role of the Product Owner (PO) and Vermont Product Team is quality assurance to ensure contract standards are achieved.

The Contractor shall perform all work required in a satisfactory manner in accordance with the requirements of the contract. The Contractor shall notify the Product Owner for appropriate action if it is likely that the Contractor will not achieve successful final delivery of the software code in accordance with the performance objectives and acceptable quality levels (AQLs) identified below.

PERFORMANCE REQUIREMENTS MATRIX

The Vermont Product Team will evaluate the performance objectives reflected below by reviews and acceptance of work products and services. As indicated, the Vermont Product Team will assess progress towards the final delivered software code. Note that the performance requirements listed below are required for the final deliverables. However, the incremental delivery of code will be assessed by the Vermont Product Team to ensure that the Contractor is on a path to successful final delivery.

Contractor Deliverable	**Contractor Performance Standards(s)**	**Contractor Acceptable Quality Level**	**State Method of Assessment**
Tested Code	Code delivered under the contract must have substantial test code coverage and a clean code base.	Minimum of 90% test coverage of all code.	Combination of manual testing and automated testing.
Properly Styled Code	GSA 18F Front End Guide for any Portal work as well as BPEL best practice in code styling for SOA and proprietary Siebel coding language.	0 linting errors and 0 warnings for any Portal work as well as Adherence to BPEL and Siebel code best practices.	Combination of manual review and automated testing.
Accessible	Web Content Accessibility Guidelines 2.1 AA (WCAG 2.1 AA) standards for any Portal work.	0 errors reported for WCAG 2.1 AA standards using an automated scanner and 0 errors reported in manual testing for any Portal work.	SoV will perform 508 compliance testing on modified Portal and Siebel pages to verify no negative impact to accessibility as a result of this work.

Deployed	Code must successfully build and deploy into testing environment(s) and must be compatible with data schemas used in production. If data schemas are not available, code must successfully build and deploy into production environment.	Successful build and deployment with deployment completion notification.	Manual review of deployment requests and combination of manual and automated testing.
Documentation	All dependencies are listed, and the licenses are documented. Major functionality in the software/source code is documented.	Individual methods are documented inline using comments that permit the use of tools such as JsDoc. System diagram is provided.	Combination of manual review and automated testing, if available.
Security Compliant	OWASP Application Security Verification Standard 3.0 and meet the requirements of an application in a CMS MARS-E compliant environment.	Code submitted must be free of medium- and high-level static and dynamic security vulnerabilities in accordance with the remediation plan as allowed under CMS MARS-E.	Manual review of application scan results by the State security team. State to document false positives and provide risk evaluation inclusive of all risk waivers to reach acceptable level of risk. Code scan remediations to be tracked in either the POAM or the Threat and Vulnerability Management (TVM) report.
User Research and Design Artifacts	Initial and subsequent user workflow design activities must be conducted and reviewed at regular intervals throughout the development process (not just at the beginning or end) to ensure the user needs are well understood and that the design solution works well for users.	Vendor shall work with the State to establish a user workflow design creation and review timeline for the project and add those to the project plan.	Participation and manual review of workflow designs.

PROCEDURES

Delivery of all software assets will occur by pull request from the Contractor's repository to the appropriate Vermont repository. If inspection results are satisfactory, the pull request will be merged; otherwise, deficiencies will be noted in the pull request or through issues as described below. The Vermont Product Team and PO may find the delivery satisfactory even though further work is required.

The Vermont Product Team will review the related functionality to ensure compliance with acceptance criteria and requirements of the user stories. All clarifications and changes to the user stories that are agreed upon are documented in the issue tracker. Incomplete or inadequate code and user stories will be noted in a mutually agreed-upon issue tracker with links to each issue shared with the PO. The Contractor may respond in that tracker as appropriate, addressing the accuracy and validity of the defect as well as any planned corrective action (if not already noted). The issue tracker will be updated as revised acceptance criteria are added to the incomplete backlog items as part of the backlog grooming process. The Contractor's team will discuss and document actions to prevent recurrence.

At the conclusion of the period of performance, the Vermont Product Team will follow a similar procedure to document discrepancies and to assess overall performance.

ACCEPTANCE OF SERVICES

The Product Owner shall review all work products for compliance with performance standards described in Attachment A, Section 26 and monitoring procedures described in this QASP. The PO shall not accept work products for the contract until all defects have been corrected.

ATTACHMENT B – PAYMENT PROVISIONS

The maximum dollar amount payable under this Contract is not intended as any form of a guaranteed amount. The Contractor will be paid for products or services actually performed as specified in Attachment A, up to the maximum allowable amount specified on page 1 of this Contract.

1. Prior to commencement of work and release of any payments, Contractor shall submit to the State:

    a. A certificate of insurance consistent with the requirements set forth in Attachment C, Section 8 (Insurance), and with any additional requirements for insurance as may be set forth elsewhere in this contract; and

    b. A current IRS Form W-9 (signed within the last six months).

2. Payment terms are NET 30 calendar days from date of invoice; payments against this Contract will comply with the State’s payment terms.

3. Invoices must be rendered on Contractor's standard billhead or official letterhead. Contractor shall submit invoicing on a monthly basis. Invoices shall reference this contract number, include date of submission, invoice number, and amount billed for each budget line and total amount billed.

4. The payment schedule for delivered services is included in this Attachment B. Contractor shall submit invoices on a template to be mutually agreed to between Contractor and the State. For each Deliverable requiring Acceptance, the State shall approve via the electronic sign-off process in a deliverable acceptance document, which shall constitute Acceptance of each individual Deliverable. For Contractor to receive the Incremental Payment Sum for the Key Deliverables (as delineated in this Attachment B), Contractor shall include the associated deliverable acceptance document signed by the State in the invoice submission.

5. Invoices shall be submitted to the State at the following address:
AHS.DVHAInvoices@vermont.gov

6. Contractor will work with State Contract Manager to have the invoice approved before sending it to the person listed above.

7. Contractor shall be paid based on documentation and itemization of work performed and included in invoicing as required by 32 V.S.A. § 463. Invoicing must contain a summary of the M&O Services and Deliverables, where the detail underlying such summary shall be as set forth herein:

    a. For M&O Services, the invoice shall reference the M&O Services fee in the applicable calendar month, along with an itemization of any Service Level Credits applicable for the month in question, where such Service Level Credits shall be calculated in accordance with Exhibit 2.
    b. For Discretionary Services, the invoice shall reference the Discretionary Service Request name and number, dates of service, and invoice amount. Discretionary services shall be invoiced based upon payment terms as set forth in the corresponding Change Request and as agreed to by the parties.

c. For Key Deliverables, the invoice shall reference the Key Deliverable Name and Number and shall include the associated deliverable acceptance document signed by the State in the invoice submission.

d. For invoices that include DDI Activities, the invoice shall reflect the portion of Contractor services that are DDI Activities as outlined in a Change Request agreed to by the parties.

8. All fees in this Contract are inclusive of expenses and travel. There will be no reimbursement of expenses for travel, mileage, meals, or any other expenses under this Contract.

9. HSEP M&O SERVICES - Contractor shall be paid for HSEP M&O Services based on the following fees:

Services	Fee
Core M&O Services: August 15, 2016 – August 14, 2018	$21,437,500.00
Core M&O Services: August 15, 2018 – August 14, 2019	$10,876,750.00
Core M&O Services: August 15, 2019 – August 14, 2020	$10,669,500.00
Core M&O Services: August 15, 2020 – August 14, 2021	$10,971,473.00
Core M&O Services: August 15, 2021 – August 14, 2023	$22,023,387.00
Discretionary Funds**	$12,000,000.00
Key Deliverables*	$6,900,000.00
Premium Processing Time and Materials Not to Exceed	$915,000.00
Total Pricing Through August 14, 2023**	$95,793,610.00

*The total fee for Key Deliverables is comprised of the $2,200,000.00 outlined in Table A, the $1,100,000.00 outlined in Table A1, the $1,800,000.00 outlined in Table A2, and the $1,800,000.00 outlined in Table A3.
**See additional details in Section 9.2 in this Attachment B.

Should the State elect to proceed with option year August 15, 2023 through August 14, 2024 the following pricing will apply:

Optional Term Pricing August 15, 2023 through August 14, 2024:

Core M&O Services: August 15, 2023 – August 14, 2024 (if elected)	$11,364,000.00
Discretionary Services Amount (July 1, 2024 – August 14, 2024)	$1,500,000.00
Key Deliverables (August 15, 2023 – August 14, 2024)	$900,000.00
Total Option Year Pricing if elected:	$13,764,000.00

9.1 Core M&O Services

a. August 15, 2016 – August 14, 2018

The monthly payment due for Core M&O Services during this period represents 1/24th of the total fixed price Contract, less the $2,200,000.00 fee associated with the Key Deliverables, said Core M&O monthly fee being payable in 24 monthly installments of $893,229.17. For partial months, payments shall be proportional to the period of performance. Payment for Core M&O Services includes Non-Key Deliverables, Reports, and Transition Deliverables, which are not tied to an Incremental Payment Sum.

b. August 15, 2018 – August 14, 2019
The monthly payment due for Core M&O Services during this period represents 12 monthly installments of $906,395.84. For partial months, payments shall be proportional to the period of performance. Payment for Core M&O Services includes Non-Key Deliverables, Reports, and Transition Deliverables, which are not tied to an Incremental Payment Sum.

c. August 15, 2019 – August 14, 2021
Core M&O Services during this period represent monthly installments of the amounts below. For partial months, payments shall be proportional to the period of performance. Payment for Core M&O Services includes Non-Key Deliverables, Reports, and Transition Deliverables, which are not tied to an Incremental Payment Sum.

i. August 15, 2019 – August 14, 2020: $889,125.00 per month
ii. August 15, 2020 – August 14, 2021: $914,289.39 per month

d. August 15, 2021 – August 14, 2023
Core M&O Services during this period represent monthly installments of the amounts below. For partial months, payments shall be proportional to the period of performance. Payment for Core M&O Services includes Non-Key Deliverables, Reports, and Transition Deliverables, which are not tied to an Incremental Payment Sum.

i. August 15, 2021 – December 31, 2021: $899,000.00 per month
ii. January 1, 2022 – August 14, 2023: $922,000.00 per month

e. August 15, 2023 – August 14, 2024 (if elected by the State via an Amendment as mutually agreed by the Parties)
Core M&O Services during this period represent monthly installments of the amounts below. For partial months, payments shall be proportional to the period of performance. Payment for Core M&O Services includes Non-Key Deliverables, Reports, and Transition Deliverables, which are not tied to an Incremental Payment Sum.

iii. August 15, 2023 – August 14, 2024: $947,000.00 per month

f. Upon State election by the process delineated in Section 8 of Attachment A the monthly payment due for Core M&O Services shall be reduced by the following amounts effective at the beginning of the next full calendar month after Contractor's shut down of the applicable Managed Application services in all environments.

i. ECM Managed Application: $25,156.25 shall be deducted per month
ii. OBIEE Managed Application: $25,156.25 shall be deducted per month
iii. Upon the time both Managed Applications are shut down the monthly installment for the applicable period in 9.1.c. and/or 9.1.d. shall be reduced by $50,132.50 per month.

9.2 Discretionary Services
Additional services not explicitly described in Attachment A, but which are approved by a Change Request as referenced in Sections 17 and 25 of Attachment A, include a Not to Exceed (NTE) amount for all such Discretionary Services of $1,500,000.00 for State Fiscal Years (SFY) SFY19, SFY22, SFY23, and SFY24, an NTE amount for all such Discretionary Services of $3,000,000.00 for SFY20, and an NTE amount for all such Discretionary Services of $3,000,000.00 for SFY21. A complete schedule of Discretionary Service funds can be found in

the table below in this Section 9.2. Regardless of the start/end date specified in the Change Request, Discretionary Services shall be funded by the Discretionary Services budget allocated for the SFY in which they were completed irrespective of when the work began. For work completed within a specific SFY, Contractor shall invoice and be paid based on the payment terms as set forth in the corresponding Change Request and as agreed to by the parties.

For work started, but not completed within an SFY, Contractor shall proceed with work into the next SFY until work is completed and provide an informational memorandum (attached hereto as Exhibit 6) to the State Authorized Representative no later than May 15th of the current SFY. Such work that spans two SFYs shall be invoiced and paid in accordance with the payment terms as set forth in the Change Request and as agreed to by the parties.

Discretionary Services	Not to Exceed
August 15, 2018 – August 14, 2019	$1,500,000.00
August 15, 2019 – June 30, 2020	$3,000,000.00
July 1, 2020 – June 30, 2021	$3,000,000.00
July 1, 2021 – June 30, 2022	$1,500,000.00
July 1, 2022 – June 30, 2023	$1,500,000.00
July 1, 2023 – June 30, 2024**	$1,500,000.00
Total	**$12,000,000.00**
July 1, 2024 – August 14, 2024 (if elected) *	$1,500,000.00

*Added to account for partial period of SFY, if August 15, 2023 – August 14, 2024 option year is elected by State.
**Discretionary Funds for this SFY are available through the Contract end date of August 14, 2023. If State executes the August 15, 2023 – August 14, 2024 option year then the Discretionary Funds for this SFY will be available through June 30, 2024.

9.3 Key Deliverables

a. Table A – Key Deliverables: (1) the Deliverable Identifier ("Del. #") Number; (2) Key Deliverable Designation; (3) the Deliverable Name; (4) the DED Submission Timeframe; (5) the Deliverable Submission Timeframe; (6) Deliverable Update Frequency; (7) Deliverable Value; and (8) Incremental Payment Sum (based on Deliverable Update Frequency).

- All DEDs for Deliverables (Key and Non-Key) require Acceptance by the State.
- All updates to Key Deliverables and all initial updates to Non-Key Deliverables require Acceptance by the State.
- All Key Deliverables (as delineated in Table A, Column 2) require Acceptance and approval via electronic sign-off by the State and Contractor. Once the State and Contractor have approved the Deliverable via electronic sign-off, Contractor shall invoice, and State shall pay the Incremental Payment Sum set forth in Table A, Column 8.

Table A: Key Deliverables (August 15, 2016 – August 14, 2018)

Del. #	Key Del.	Deliverable Name	DED Submission Timeframe	Deliverable Submission Timeframe	Deliverable Update Frequency	Deliverable Value	Incremental Payment Sum (based on Update Deliverable Frequency)
1.K01	Yes	Project Management Plan	3 Weeks after Contract Effective Date	4 Weeks after DED Approval	annually	$200,000.00	$100,000.00
1.K02	Yes	Disaster Recovery Plan	3 Weeks after Contract Effective Date	4 Weeks after DED Approval	annually	$200,000.00	$100,000.00
1.K03	Yes	M&O Manual	3 Weeks after Contract Effective Date	4 Weeks after DED Approval	quarterly	$300,000.00	$37,500.00
1.K04	Yes	M&O Schedule	3 weeks after Contract Effective Date	4 Weeks after DED Approval	monthly	$300,000.00	$12,500.00
1.K05	Yes	Architecture Document	6 weeks after Contract Effective Date	4 Weeks after DED Approval	every 6 months	$300,000.00	$75,000.00
1.K06	Yes	Availability Plan	6 weeks after Contract Effective Date	4 Weeks after DED Approval	quarterly	$300,000.00	$37,500.00
1.K07	Yes	Configuration Management Plan	9 weeks after Contract Effective Date	4 Weeks after DED Approval	quarterly	$300,000.00	$37,500.00
1.K08	Yes	SSP (State Security Plan)	16 weeks after Contract Effective Date	4 Weeks after DED Approval	quarterly	$300,000.00	$37,500.00

b. Table A1 – Key Deliverables: (1) the Deliverable Identifier ("Del. #") Number; (2) Key Deliverable Designation; (3) the Deliverable Name; (4) Deliverable Update Frequency; (5) Deliverable Value; and (6) Incremental Payment Sum (based on Deliverable Update Frequency).

Table A1: Key Deliverables – (August 15, 2018 – August 14, 2019)

Del. #	Key Del.	Deliverable Name	Deliverable Update Frequency	Estimated Deliverable Update Schedule	Deliverable Value	Incremental Payment Sum (based on Update Deliverable Frequency)
1.K01	Yes	Project Management Plan	annually	D-01.3 – 11/01/2018	$100,000.00	$100,000.00
1.K02	Yes	Disaster Recovery Plan	annually	D-02.3 – 11/01/2018	$100,000.00	$100,000.00
1.K03	Yes	M&O Manual	quarterly	D-03.9 – 10/01/2018 D-03.10 – 01/01/2019 D-03.11 – 04/01/2019 D-03.12 – 07/01/2019	$150,000.00	$37,500.00
1.K04	Yes	M&O Schedule	monthly	D-04.25 – 09/01/2018 D-04.26 – 10/01/2018 D-04.27 – 11/01/2018 D-04.28 – 12/01/2018	$150,000.00	$12,500.00

				D-04.29 – 01/01/2019 D-04.30 – 02/01/2019 D-04.31 – 03/01/2019 D-04.32 – 04/01/2019 D-04.33 – 05/01/2019 D-04.34 – 06/01/2019 D-04.35 – 07/01/2019 D-04.36 – 08/01/2019		
1.K05	Yes	Architecture Document	every 6 months	D-05.5 – 12/01/2018 D-05.6 – 06/01/2019	$150,000.00	$75,000.00
1.K06	Yes	Availability Plan	quarterly	D-06.9 – 10/01/2018 D-06.10 – 01/01/2019 D-06.11 – 04/01/2019 D-06.12 – 07/01/2019	$150,000.00	$37,500.00
1.K07	Yes	Configuration Management Plan	quarterly	D-07.9 – 10/01/2018 D-07.10 – 01/01/2019 D-07.11 – 04/01/2019 D-07.12 – 07/01/2019	$150,000.00	$37,500.00
1.K08	Yes	SSP (State Security Plan)	quarterly	D-08.9 – 11/01/2018 D-08.10 – 02/01/2019 D-08.11 – 05/01/2019 D-08.12 – 08/01/2019	$150,000.00	$37,500.00

c. Table A2 – Key Deliverables: (1) the Deliverable Identifier ("Del. #") Number; (2) Key Deliverable Designation; (3) the Deliverable Name; (4) Deliverable Update Frequency; (5) Deliverable Value; and (6) Incremental Payment Sum (based on Deliverable Update Frequency).

Table A2: Key Deliverables – (August 15, 2019 – August 14, 2021)

Del. #	Key Del.	Deliverable Name	Deliverable Update Frequency	Estimated Deliverable Update Schedule	Deliverable Value	Incremental Payment Sum (based on Deliverable Update Frequency)
1.K02	Yes	Disaster Recovery Plan	annually	D-02.04 – 11/01/2019 D-02.05 – 11/01/2020	$200,000.00	$100,000.00
1.K03	Yes	M&O Manual	every 6 months	D-03.13 – 10/01/2019 D-03.14 – 04/01/2020 D-03.15 – 10/01/2020 D-03.16 – 04/01/2021	$480,000.00	$120,000.00
1.K05	Yes	Architecture Document	every 6 months	D-05.07 – 12/01/2019 D-05.08 – 06/01/2020 D-05.09 – 12/01/2020 D-05.10 – 06/01/2021	$480,000.00	$120,000.00
1.K06	Yes	Availability Plan	annually	D-06.13 – 05/01/2020 D-06.14 – 05/01/2021	$200,000.00	$100,000.00
1.K07	Yes	Configuration Management Plan	annually	D-07.13 – 05/01/2020	$200,000.00	$100,000.00

				D-07.14 – 05/01/2021		
1.K08	Yes	SSP (State Security Plan)	quarterly	D-08.13 – 11/01/2019 D-08.14 – 02/01/2020 D-08.15 – 05/01/2020 D-08.16 – 08/01/2020 D-08.17 – 11/01/2020 D-08.18 – 02/01/2021 D-08.19 – 05/01/2021 D-08.20 – 08/01/2021	$240,000.00	$30,000.00

d. Table A3 – Key Deliverables: (1) the Deliverable Identifier ("Del. #") Number; (2) Key Deliverable Designation; (3) the Deliverable Name; (4) Deliverable Update Frequency; (5) Deliverable Value; and (6) Incremental Payment Sum (based on Deliverable Update Frequency).

Table A3: Key Deliverables – (August 15, 2021 – August 14, 2023)

Del. #	Key Del.	Deliverable Name	Deliverable Update Frequency	Estimated Deliverable Update Schedule	Deliverable Value	Incremental Payment Sum (based on Deliverable Update Frequency)
1.K02	Yes	Disaster Recovery Plan	annually	D-02.06 – 11/01/2021 D-02.07 – 11/01/2022	$200,000.00	$100,000.00
1.K03	Yes	M&O Manual	every 6 months	D-03.17 – 10/01/2021 D-03.18 – 04/01/2022 D-03.19 – 10/01/2022 D-03.20 – 04/01/2023	$480,000.00	$120,000.00
1.K05	Yes	Architecture Document	every 6 months	D-05.11 – 12/01/2021 D-05.12 – 06/01/2022 D-05.13 – 12/01/2022 D-05.14 – 06/01/2023	$480,000.00	$120,000.00
1.K06	Yes	Availability Plan	annually	D-06.15 – 05/01/2022 D-06.16 – 05/01/2023	$200,000.00	$100,000.00
1.K07	Yes	Configuration Management Plan	annually	D-07.15 – 05/01/2022 D-07.16 – 05/01/2023	$200,000.00	$100,000.00
1.K08	Yes	SSP (State Security Plan)	quarterly	D-08.21 – 11/01/2021 D-08.22 – 02/01/2022 D-08.23 – 05/01/2022 D-08.24 – 08/01/2022 D-08.25 – 11/01/2022 D-08.26 – 02/01/2023 D-08.27 – 05/01/2023 D-08.28 – 08/01/2023	$240,000.00	$30,000.00

a. Table A4 – Key Deliverables: (1) the Deliverable Identifier ("Del. #") Number; (2) Key Deliverable Designation; (3) the Deliverable Name; (4) Deliverable Update Frequency; (5) Deliverable Value; and (6) Incremental Payment Sum (based on Deliverable Update Frequency).

Table A4: Key Deliverables – (August 15, 2023 – August 14, 2024) (if elected)

Del. #	Key Del.	Deliverable Name	Deliverable Update Frequency	Estimated Deliverable Update Schedule	Deliverable Value	Incremental Payment Sum (based on Deliverable Update Frequency)
1.K02	Yes	Disaster Recovery Plan	annually	D-02.08 – 11/01/2023	$100,000.00	$100,000.00
1.K03	Yes	M&O Manual	every 6 months	D-03.21 – 10/01/2023 D-03.22 – 04/01/2024	$240,000.00	$120,000.00
1.K05	Yes	Architecture Document	every 6 months	D-05.15 – 12/01/2023 D-05.16 – 06/01/2024	$240,000.00	$120,000.00
1.K06	Yes	Availability Plan	annually	D-06.17 – 05/01/2024	$100,000.00	$100,000.00
1.K07	Yes	Configuration Management Plan	annually	D-07.17 – 05/01/2024	$100,000.00	$100,000.00
1.K08	Yes	SSP (State Security Plan)	quarterly	D-08.29 – 11/01/2023 D-08.30 – 02/01/2024 D-08.31 – 05/01/2024 D-08.32 – 08/01/2024	$120,000.00	$30,000.00

e. It is understood and agreed that:

- Where applicable, the content of all Deliverables delineated in Table A, Table A1, Table A2, and Table A3 of this Attachment B shall be based upon, and therefore substantially similar to, the versions of the Deliverables previously delivered to State by Contractor.
- All timelines set forth in Table A of this Attachment B are dependent on Contractor and State adhering to Attachment A, Sections 13, 14 and 15: DED Review and Approval Process, DED Revision Process, and Deliverables Review and Approval Process.
- Notwithstanding the DED Submission Timeframe set forth in Attachment B, Table A above, in the event the Contactor has already drafted a DED that the State has accepted for a specific Deliverable, Contractor will present the existing DED to State in accordance with Attachment A, Section 12 Existing Deliverables/DED Catalog Review within 2 weeks of Contract execution. Upon the State's Acceptance of the existing DED, the timeframe set forth in the Deliverable Submission Timeframe shall commence.
- If the first submission of a monthly or quarterly Deliverable does not align with start of a calendar month or quarter, Contractor shall align the subsequent deliveries with the first of the calendar month or quarterly respectively.
- In the event a DED is not accepted by the State in the timelines in the above Table A of this Attachment B, due to a State Delay, the value associated with the associated Deliverable any outstanding incremental payments tied to the Deliverable will be paid upon Acceptance of the Deliverable in the subsequent payment.
- In the event a DED is not accepted by the State in the timelines in the above Table A of this Attachment B, due to reasons other than a State Delay, the value associated

with the associated Deliverable such incremental payments will be redistributed among the remaining Incremental Payment Sums.

- Attachment B, Table A1 Key Deliverables shall continue the existing schedule as set forth in Table A of this Attachment B which are estimated dates and may be updated as agreed upon via the M&O Schedule.
- Attachment B, Table A2 Key Deliverables establishes a new Update Frequency and Update Schedule. Table A3 Key Deliverables shall continue the schedule set forth in Table A2 of this Attachment B which are estimated dates and may be updated as mutually agreed upon by the Parties.

9.4 Premium Processing Development Time and Materials

a. Contractor shall provide dedicated and part-time resources as needed to provide the services during the period of performance as described in Attachment A, Section 26 Premium Processing Development.

b. Contractor shall invoice on a time and materials basis against the previously executed CR-046 until $150,000.00 is expended.

c. Upon expiration of the $150,000.00 funding from CR-046, CR-046 shall expire. Contractor shall then continue to perform in accordance with this Contract, whereupon, Contactor shall begin invoicing on a time and materials basis, up to a maximum of $915,000.00 or until September 30, 2021, whichever occurs first, in accordance with Amendment No. 4, Attachment A, Section 26 and Attachment B, Rate Card in Table 9.4 Premium Processing Rate Card below.

d. Invoices shall reference Attachment A, Section 26 Premium Processing and include service dates, description, rate, and hours worked.

e. Contractor shall retain full discretion over the assignment of its staff in the execution of work requested under Attachment A, Section 26 Premium Processing.

f. Contractor shall provide services based on the Role Descriptions listed in Table 9.4. Resources may perform tasks including but not limited to those listed in the Role Description column.

g. Contractor shall provide hourly support at the rates listed in Table 9.4.

Table 9.4 Premium Processing Rate Card

Billing Role	Role Description	CY20 Hourly Rate	CY21 Hourly Rate
Analyst Level 3	• Provides technical writing and analysis for project deliverables; and • Assists in the production and organization of work products.	$122	$126
Analyst Level 4	• Participates in the identification and analysis of functional and technical requirements; and • Produces detailed software design specifications and related artifacts for developers.	$150	$155

Analyst Level 5	• Provides leadership and guidance to functional and technical resources regarding project deliverables and work products; and • Consults on the design of business and system architecture.	$190	$196
Design Development Engineer Level 2	• Performs basic development for software solutions.	$137	$141
Design Development Engineer Level 3	• Performs development for software solutions; and • Consults on technical designs according to industry standards and best practices.	$183	$188
Design Development Engineer Level 4	• Applies principles of software engineering to lead the development of software solutions; and • Provides oversight of software coding standards and practices.	$211	$217
Design Development Engineer Level 6	• Directs development team and provides leadership and guidance to functional and technical resources regarding project deliverables and work product; and • Provides strategic direction and oversight on the design of business and system architecture.	$272	$280
Senior Program Administration Specialist	• Provides project management support.	$143	147
Project Manager	• Applies programmatic oversight and ensures project management principles are leveraged throughout; and • Manages project scope, schedule, and budget through CR lifecycle.	$245	$252
Senior Comp Security Systems Specialist	• Applies security principles to inform the design and development of software solutions; and • Provides oversight of software coding standards and practices.	$190	$196
Quality Assurance Specialist	• Participates in the identification and analysis of functional and technical requirements; and • Assists in the execution of test cases.	$122	$126
Quality Assurance Manager	• Provides overall direction for quality management; and • Assists in the planning and execution of test cases.	$150	$155

Attachment F
AGENCY OF HUMAN SERVICES' CUSTOMARY CONTRACT PROVISIONS

1. **Definitions:** For purposes of this Attachment F, the term "Agreement" shall mean the form of the contract or grant, with all of its parts, into which this Attachment F is incorporated. The meaning of the term "Party" when used in this Attachment F shall mean any named party to this Agreement *other than* the State of Vermont, the Agency of Human Services (AHS) and any of the departments, boards, offices and business units named in this Agreement. As such, the term "Party" shall mean, when used in this Attachment F, the Contractor or Grantee with whom the State of Vermont is executing this Agreement. If Party, when permitted to do so under this Agreement, seeks by way of any subcontract, sub-grant or other form of provider agreement to employ any other person or entity to perform any of the obligations of Party under this Agreement, Party shall be obligated to ensure that all terms of this Attachment F are followed. As such, the term "Party" as used herein shall also be construed as applicable to, and describing the obligations of, any subcontractor, sub-recipient or sub-grantee of this Agreement. Any such use or construction of the term "Party" shall not, however, give any subcontractor, sub-recipient or sub-grantee any substantive right in this Agreement without an express written agreement to that effect by the State of Vermont.

2. **Agency of Human Services**: The Agency of Human Services is responsible for overseeing all contracts and grants entered by any of its departments, boards, offices and business units, however denominated. The Agency of Human Services, through the business office of the Office of the Secretary, and through its Field Services Directors, will share with any named AHS-associated party to this Agreement oversight, monitoring and enforcement responsibilities. Party agrees to cooperate with both the named AHS-associated party to this contract and with the Agency of Human Services itself with respect to the resolution of any issues relating to the performance and interpretation of this Agreement, payment matters and legal compliance.

3. **Medicaid Program Parties** (*applicable to any Party providing services and supports paid for under Vermont's Medicaid program and Vermont's Global Commitment to Health Waiver*):

   Inspection and Retention of Records: In addition to any other requirement under this Agreement or at law, Party must fulfill all state and federal legal requirements, and will comply with all requests appropriate to enable the Agency of Human Services, the U.S. Department of Health and Human Services (along with its Inspector General and the Centers for Medicare and Medicaid Services), the Comptroller General, the Government Accounting Office, or any of their designees: (i) to evaluate through inspection or other means the quality, appropriateness, and timeliness of services performed under this Agreement; and (ii) to inspect and audit any records, financial data, contracts, computer or other electronic systems of Party relating to the performance of services under Vermont's Medicaid program and Vermont's Global Commitment to Health Waiver. Party will retain for ten years all documents required to be retained pursuant to 42 CFR 438.3(u).

   Subcontracting for Medicaid Services: Notwithstanding any permitted subcontracting of services to be performed under this Agreement, Party shall remain responsible for ensuring that this Agreement is fully performed according to its terms, that subcontractor remains in compliance with the terms hereof, and that subcontractor complies with all state and federal laws and regulations relating to the Medicaid program in Vermont. Subcontracts, and any service provider agreements entered into by Party in connection with the performance of this Agreement, must clearly specify in writing the responsibilities of the subcontractor or other service provider and Party must retain the authority to revoke its subcontract or service provider agreement or to impose other sanctions if the performance of the subcontractor or service provider is inadequate or if its performance deviates from any requirement of this Agreement. Party shall make available on request all contracts, subcontracts and service provider agreements between the Party, subcontractors and other service providers to the Agency of Human Services and any of its departments as well as to the Center for Medicare and Medicaid Services.

Medicaid Notification of Termination Requirements: Party shall follow the Department of Vermont Health Access Managed-Care-Organization enrollee-notification requirements, to include the requirement that Party provide timely notice of any termination of its practice.

Encounter Data: Party shall provide encounter data to the Agency of Human Services and/or its departments and ensure further that the data and services provided can be linked to and supported by enrollee eligibility files maintained by the State.

Federal Medicaid System Security Requirements Compliance: Party shall provide a security plan, risk assessment, and security controls review document within three months of the start date of this Agreement (and update it annually thereafter) in order to support audit compliance with 45 CFR 95.621 subpart F, *ADP System Security Requirements and Review Process*.

4. **Workplace Violence Prevention and Crisis Response** (*applicable to any Party and any subcontractors and sub-grantees whose employees or other service providers deliver social or mental health services directly to individual recipients of such services*):

   Party shall establish a written workplace violence prevention and crisis response policy meeting the requirements of Act 109 (2016), 33 VSA §8201(b), for the benefit of employees delivering direct social or mental health services. Party shall, in preparing its policy, consult with the guidelines promulgated by the U.S. Occupational Safety and Health Administration for *Preventing Workplace Violence for Healthcare and Social Services Workers*, as those guidelines may from time to time be amended.

   Party, through its violence protection and crisis response committee, shall evaluate the efficacy of its policy, and update the policy as appropriate, at least annually. The policy and any written evaluations thereof shall be provided to employees delivering direct social or mental health services.

   Party will ensure that any subcontractor and sub-grantee who hires employees (or contracts with service providers) who deliver social or mental health services directly to individual recipients of such services, complies with all requirements of this Section.

5. **Non-Discrimination**:
   Party shall not discriminate, and will prohibit its employees, agents, subcontractors, sub-grantees and other service providers from discrimination, on the basis of age under the Age Discrimination Act of 1975, on the basis of handicap under section 504 of the Rehabilitation Act of 1973, on the basis of sex under Title IX of the Education Amendments of 1972, and on the basis of race, color or national origin under Title VI of the Civil Rights Act of 1964. Party shall not refuse, withhold from or deny to any person the benefit of services, facilities, goods, privileges, advantages, or benefits of public accommodation on the basis of disability, race, creed, color, national origin, marital status, sex, sexual orientation or gender identity as provided by Title 9 V.S.A. Chapter 139.

   No person shall on the grounds of religion or on the grounds of sex (including, on the grounds that a woman is pregnant), be excluded from participation in, be denied the benefits of, or be subjected to discrimination, to include sexual harassment, under any program or activity supported by State of Vermont and/or federal funds.

   Party further shall comply with the non-discrimination requirements of Title VI of the Civil Rights Act of 1964, 42 USC Section 2000d, et seq., and with the federal guidelines promulgated pursuant to Executive Order 13166 of 2000, requiring that contractors and subcontractors receiving federal funds assure that persons with limited English proficiency can meaningfully access services. To the extent Party provides assistance to individuals with limited English proficiency through the use of oral or written translation or interpretive services, such individuals cannot be required to pay for such services.

6. **Employees and Independent Contractors**:
Party agrees that it shall comply with the laws of the State of Vermont with respect to the appropriate classification of its workers and service providers as "employees" and "independent contractors" for all purposes, to include for purposes related to unemployment compensation insurance and workers compensation coverage, and proper payment and reporting of wages. Party agrees to ensure that all of its subcontractors or sub-grantees also remain in legal compliance as to the appropriate classification of "workers" and "independent contractors" relating to unemployment compensation insurance and workers compensation coverage, and proper payment and reporting of wages. Party will on request provide to the Agency of Human Services information pertaining to the classification of its employees to include the basis for the classification. Failure to comply with these obligations may result in termination of this Agreement.

7. **Data Protection and Privacy:**
Protected Health Information: Party shall maintain the privacy and security of all individually identifiable health information acquired by or provided to it as a part of the performance of this Agreement. Party shall follow federal and state law relating to privacy and security of individually identifiable health information as applicable, including the Health Insurance Portability and Accountability Act (HIPAA) and its federal regulations.

Substance Abuse Treatment Information: Substance abuse treatment information shall be maintained in compliance with 42 C.F.R. Part 2 if the Party or subcontractor(s) are Part 2 covered programs, or if substance abuse treatment information is received from a Part 2 covered program by the Party or subcontractor(s).

Protection of Personal Information: Party agrees to comply with all applicable state and federal statutes to assure protection and security of personal information, or of any personally identifiable information (PII), including the Security Breach Notice Act, 9 V.S.A. § 2435, the Social Security Number Protection Act, 9 V.S.A. § 2440, the Document Safe Destruction Act, 9 V.S.A. § 2445 and 45 CFR 155.260. As used here, PII shall include any information, in any medium, including electronic, which can be used to distinguish or trace an individual's identity, such as his/her name, social security number, biometric records, etc., either alone or when combined with any other personal or identifiable information that is linked or linkable to a specific person, such as date and place or birth, mother's maiden name, etc.

Other Confidential Consumer Information: Party agrees to comply with the requirements of AHS Rule No. 08-048 concerning access to and uses of personal information relating to any beneficiary or recipient of goods, services or other forms of support. Party further agrees to comply with any applicable Vermont State Statute and other regulations respecting the right to individual privacy. Party shall ensure that all of its employees, subcontractors and other service providers performing services under this agreement understand and preserve the sensitive, confidential and non-public nature of information to which they may have access.

Data Breaches: Party shall report to AHS, though its Chief Information Officer (CIO), any impermissible use or disclosure that compromises the security, confidentiality or privacy of any form of protected personal information identified above within 24 hours of the discovery of the breach. Party shall in addition comply with any other data breach notification requirements required under federal or state law.

8. **Abuse and Neglect of Children and Vulnerable Adults:**
Abuse Registry. Party agrees not to employ any individual, to use any volunteer or other service provider, or to otherwise provide reimbursement to any individual who in the performance of services connected with this agreement provides care, custody, treatment, transportation, or supervision to children or to vulnerable adults if there has been a substantiation of abuse or neglect or exploitation involving that individual. Party is responsible for confirming as to each individual having such contact with children or vulnerable adults the non-existence of a substantiated allegation of abuse, neglect or exploitation by verifying that fact though (a) as to vulnerable adults, the Adult Abuse Registry maintained by the Department of Disabilities, Aging and Independent Living and (b) as to children, the Central Child Protection Registry (unless the Party holds a valid child care license or registration from the Division of Child Development, Department for Children and Families). See 33 V.S.A. §4919(a)(3) and 33 V.S.A. §6911(c)(3).

Reporting of Abuse, Neglect, or Exploitation. Consistent with provisions of 33 V.S.A. §4913(a) and §6903, Party and any of its agents or employees who, in the performance of services connected with this agreement, (a) is a caregiver or has any other contact with clients and (b) has reasonable cause to believe that a child or vulnerable adult has been abused or neglected as defined in Chapter 49 or abused, neglected, or exploited as defined in Chapter 69 of Title 33 V.S.A. shall: as to children, make a report containing the information required by 33 V.S.A. §4914 to the Commissioner of the Department for Children and Families within 24 hours; or, as to a vulnerable adult, make a report containing the information required by 33 V.S.A. §6904 to the Division of Licensing and Protection at the Department of Disabilities, Aging, and Independent Living within 48 hours. Party will ensure that its agents or employees receive training on the reporting of abuse or neglect to children and abuse, neglect or exploitation of vulnerable adults.

9. **Information Technology Systems**:
Computing and Communication: Party shall select, in consultation with the Agency of Human Services' Information Technology unit, one of the approved methods for secure access to the State's systems and data, if required. Approved methods are based on the type of work performed by the Party as part of this agreement. Options include, but are not limited to:
    1. Party's provision of certified computing equipment, peripherals and mobile devices, on a separate Party's network with separate internet access. The Agency of Human Services' accounts may or may not be provided.
    2. State supplied and managed equipment and accounts to access state applications and data, including State issued active directory accounts and application specific accounts, which follow the National Institutes of Standards and Technology (NIST) security and the Health Insurance Portability & Accountability Act (HIPAA) standards.

***Intellectual Property/Work Product Ownership*:** All data, technical information, materials first gathered, originated, developed, prepared, or obtained as a condition of this agreement and used in the performance of this agreement -- including, but not limited to all reports, surveys, plans, charts, literature, brochures, mailings, recordings (video or audio), pictures, drawings, analyses, graphic representations, software computer programs and accompanying documentation and printouts, notes and memoranda, written procedures and documents, which are prepared for or obtained specifically for this agreement, or are a result of the services required under this grant -- shall be considered "work for hire" and remain the property of the State of Vermont, regardless of the state of completion unless otherwise specified in this agreement. Such items shall be delivered to the State of Vermont upon 30-days notice by the State. With respect to software computer programs and / or source codes first developed for the State, all the work shall be considered "work for hire," i.e., the State, not the Party (or subcontractor or sub-grantee), shall have full and complete ownership of all software computer programs, documentation and/or source codes developed.

Party shall not sell or copyright a work product or item produced under this agreement without explicit permission from the State of Vermont.

If Party is operating a system or application on behalf of the State of Vermont, Party shall not make information entered into the system or application available for uses by any other party than the State of Vermont, without prior authorization by the State. Nothing herein shall entitle the State to pre-existing Party's materials.

Party acknowledges and agrees that should this agreement be in support of the State's implementation of the Patient Protection and Affordable Care Act of 2010, Party is subject to the certain property rights provisions of the Code of Federal Regulations and a Grant from the Department of Health and Human Services, Centers for Medicare & Medicaid Services. Such agreement will be subject to, and incorporates here by reference, 45 CFR 74.36, 45 CFR 92.34 and 45 CFR 95.617 governing rights to intangible property.

Security and Data Transfers: Party shall comply with all applicable State and Agency of Human Services' policies and standards, especially those related to privacy and security. The State will advise the Party of any new policies, procedures, or protocols developed during the term of this agreement as they are issued and will work with the Party to implement any required.

Party will ensure the physical and data security associated with computer equipment, including desktops, notebooks, and other portable devices, used in connection with this Agreement. Party will also assure that any media or mechanism used to store or transfer data to or from the State includes industry standard security mechanisms such as continually up-to-date malware protection and encryption. Party will make every reasonable effort to ensure media or data files transferred to the State are virus and spyware free. At the conclusion of this agreement and after successful delivery of the data to the State, Party shall securely delete data (including archival backups) from Party's equipment that contains individually identifiable records, in accordance with standards adopted by the Agency of Human Services.

Party, in the event of a data breach, shall comply with the terms of Section 7 above.

10. **Other Provisions**:
Environmental Tobacco Smoke. Public Law 103-227 (also known as the Pro-Children Act of 1994) and Vermont's Act 135 (2014) (An act relating to smoking in lodging establishments, hospitals, and child care facilities, and on State lands) restrict the use of tobacco products in certain settings. Party shall ensure that no person is permitted: (i) to use tobacco products or tobacco substitutes as defined in 7 V.S.A. § 1001 on the premises, both indoor and outdoor, of any licensed child care center or afterschool program at any time; (ii) to use tobacco products or tobacco substitutes on the premises, both indoor and in any outdoor area designated for child care, health or day care services, kindergarten, pre-kindergarten, elementary, or secondary education or library services; and (iii) to use tobacco products or tobacco substitutes on the premises of a licensed or registered family child care home while children are present and in care. Party will refrain from promoting the use of tobacco products for all clients and from making tobacco products available to minors.

Failure to comply with the provisions of the federal law may result in the imposition of a civil monetary penalty of up to $1,000 for each violation and/or the imposition of an administrative compliance order on the responsible entity. The federal Pro-Children Act of 1994, however, does not apply to portions of facilities used for inpatient drug or alcohol treatment; service providers whose sole source of applicable federal funds is Medicare or Medicaid; or facilities where Women, Infants, & Children (WIC) coupons are redeemed.

2-1-1 Database: If Party provides health or human services within Vermont, or if Party provides such services near the Vermont border readily accessible to residents of Vermont, Party shall adhere to the "Inclusion/Exclusion" policy of Vermont's United Way/Vermont 211 (Vermont 211), and will provide to Vermont 211 relevant descriptive information regarding its agency, programs and/or contact information as well as accurate and up to date information to its database as requested. The "Inclusion/Exclusion" policy can be found at www.vermont211.org.

Voter Registration: When designated by the Secretary of State, Party agrees to become a voter registration agency as defined by 17 V.S.A. §2103 (41), and to comply with the requirements of state and federal law pertaining to such agencies.

Drug Free Workplace Act: Party will assure a drug-free workplace in accordance with 45 CFR Part 76.

Lobbying: No federal funds under this agreement may be used to influence or attempt 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 the awarding of any federal contract, continuation, renewal, amendments other than federal appropriated funds.

ATTACHMENT G

MODIFICATION OF CUSTOMARY PROVISIONS OF ATTACHMENT F

1. **Requirements of Sections in Attachment F are hereby modified:**

A. **Notwithstanding Section 3 Medicaid Program Parties, the following subsection, Medicaid Notification of Termination Requirements, is not applicable under this Contract:**

Medicaid Notification of Termination Requirements: Party shall follow the Department of Vermont Health Access Managed-Care-Organization enrollee-notification requirements, to include the requirement that Party provide timely notice of any termination of its practice.

B. **Notwithstanding Section 3 Medicaid Program Parties, the following subsection, Encounter Data is modified as follows:**

Encounter Data: Party shall provide State of Vermont, Agency of Human Services' encounter data back to the Agency of Human Services and/or its departments and ensure further that the data and services provided can be linked to and supported by enrollee eligibility files maintained by the State.

C. **Notwithstanding Section 7 Data Protection and Privacy of Attachment F, the following section, Protected Health Information, is hereby deleted and replaced as follows:**

Protected Health Information("PHI"). Party shall maintain the privacy and security of all PHI in accordance with the obligations contained in Attachment E (Business Associate Agreement).

D. **Notwithstanding Section 7 Data Breaches of Attachment F, the following subsection, Data Breaches, is hereby deleted and replaced as follows:**

Data Breaches: Party shall report data breaches of PHI in accordance with the provisions of Attachment E (Business Associate Agreement). Party shall report to AHS, though its Chief Information Officer (CIO), any impermissible use or disclosure that compromises the security, confidentiality, or privacy of any form of protected personal information identified as soon possible but no later than five business days of the discovery of the breach. Party shall in addition comply with any other data breach notification requirements required under federal or state law.