

**Amended and Restated Contract.** As of August 15, 2016, the State and the Contractor originally entered into this contract (the “Original Contract”). As of August 15, 2018, the State and the Contractor agree to amend and restate the Original Contract to read in whole as set forth in this first amendment to the Original Contract. The parties hereby affirm each of their respective representations and certifications made as of the date of the Original Contract.

**1. Parties:** This contract (“Contract”) is an amendment and restatement in its entirety of the contract for services #31750 between the State of Vermont, Department of Vermont Health Access (hereafter called “State”) and OptumInsight, Inc., with a principal place of business in Eden Prairie, Minnesota (hereafter called “Contractor”). Contractor’s form of business organization is a corporation. It is the Contractor’s responsibility to contact the Vermont Department of Taxes to determine if, by law, the Contractor is required to have a Vermont Department of Taxes Business Account Number.

**2. Subject Matter:** 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), non-recurring work required to transition to a new IT Service management (ITSM) software platform, and the creation of certain documentation deliverables required for any future potential transition to a successor M&O provider.

**3. Maximum Amount:** In consideration of the services to be performed by Contractor, the State agrees to pay Contractor, in accordance with the payment provisions specified in Attachment B, a sum not to exceed \$37,114,250.00 (the “Maximum Amount”).

**4. Contract Term:** The period of Contractor’s performance shall begin on August 15, 2016 (“Effective Date”) and end on August 14, 2019. The State has the option of renewing this Contract with Contractor, for up to one (1) additional one (1) year extension.

**5. Prior Approvals:** This Contract shall not be binding unless and until all requisite prior approvals have been obtained in accordance with current State law, bulletins, and interpretations.

**6. Amendment:** No changes, modifications, or amendments in the terms and conditions of this Contract shall be effective unless reduced to writing, numbered and signed by the duly authorized representative of the State and Contractor.

**7. Cancellation:** This Contract may be cancelled by Contractor by giving written notice to State at least 180 days in advance. This Contract may be cancelled by State by giving written notice to Contractor at least 180 days in advance.

**8. Attachments:** This Contract consists of 129 pages including the following attachments which are incorporated herein (“Contract Documents”):

Attachment A – Specification of Work

- Exhibit 1 – State Requirements and Contractor’s Responsibilities listed by Service
- Exhibit 2 – Service Level Agreements and Service Level Credits
- Exhibit 3 – Security Policies

Attachment B – Payment Provisions

Attachment C – Standard State Provisions for Contracts and Grants (revision date December 15, 2017)

Attachment D – Other Terms and Conditions

Attachment E – Business Associate Agreement

Appendix I – Subcontractor Compliance Form

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

- 1) This document
- 2) Attachment D (Other Terms and Conditions)
- 3) Attachment C (Standard State Provisions for Contracts and Grants)
- 4) Attachment A (with Exhibits)
- 5) Attachment B
- 6) Attachment E
- 7) Other attachments (if applicable)

**WE THE UNDERSIGNED PARTIES AGREE TO BE BOUND BY THIS CONTRACT:**

**BY THE STATE OF VERMONT:**

e-Signed by Cory Gustafson  
on 2018-08-22 01:15:25 GMT

Cory Gustafson  
Commissioner  
Department of Vermont Health Access  
NOB 1 South  
280 State Drive  
Waterbury, VT 05671-1010  
Phone: 802-241-0246  
Email: [Cory.Gustafson@vermont.gov](mailto:Cory.Gustafson@vermont.gov)

**BY THE CONTRACTOR:**

e-Signed by Paul Miller  
on 2018-08-21 18:12:55 GMT

Paul M. Miller  
Vice President Finance  
Optum Corporate Finance  
OptumInsight, Inc.  
11000 Optum Circle  
Eden Prairie, MN 55344  
Phone: 952-205-6089  
Email: [paul.m.miller@optum.com](mailto:paul.m.miller@optum.com)

**ATTACHMENT A  
SPECIFICATIONS OF WORK TO BE PERFORMED**

**1. THE CONTACTS FOR THIS CONTRACT ARE AS FOLLOWS:**

	<b>State Fiscal Manager</b>	<b>Authorized State Representative</b>	<b>For the Contractor</b>
<b>Name:</b>	Susan Whitney	Darin Prail	Lynn Willenbring
<b>Phone:</b>	(802) 241-0258	(802) 338-5719	(952) 205-4873
<b>E-Mail:</b>	Susan.Whitney@vermont.gov	Darin.Prail@vermont.gov	<a href="mailto:Lynn.Willenbring@optum.com">Lynn.Willenbring@optum.com</a>

**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	<a href="mailto:ahs.dvhalegal@vermont.gov">ahs.dvhalegal@vermont.gov</a>	<a href="mailto:aimee.blatz@optum.com">aimee.blatz@optum.com</a>

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
  - 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, Table 1 - Managed Applications, Contractor will provide a range of services which are enumerated in Section 6.1, Table 2 – Core M&O Services in Scope, and set forth in greater detail in Exhibit 1 to this Attachment A ("Core M&O Services").

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”)**

		<b>HSEP Managed Applications</b>
1.		Master Data Management
2.		Notification Engine
3.		Access Integration
4.		Enterprise Content Management
5.		Rules Engine (OPA)
6.		Identity and Access Management (OAM Suite)
7.		Existing Integrations and interfaces between HSEP and External Systems
8.		Web Analytics
9.		Portal (Liferay)
10.		Business Intelligence (OBIEE)
11.		Workflow Management
12.		Database Services
13.		Siebel (Case Management)
14.		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**

<b>FUNCTIONAL AREAS AND SUB-AREAS</b>
<b>Application Maintenance and Operation Services</b>
• Managed Application Support
• Corrective and Emergency Maintenance
• Preventive Maintenance
• Adaptive Maintenance
• Application Maintenance Tuning
• Application Quality Assurance
• Automated Regression Test Suite
• 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
<b>Availability Management</b>
<b>Capacity Management</b>
<b>DBMS and Clusterware Services</b>
<b>Disaster Recovery</b>
<b>Enterprise Content Management</b>
<b>Escalation Management</b>
<b>Event Management/Monitoring</b>
<b>Identity and Access Management</b>
<b>Knowledge Management</b>
<b>MDM and ACCESS Integration Services</b>
<b>Release Management</b>
<b>Request Services</b>
• Service Desk Services
• Service Desk Support
• IT Service Management (ITSM) Services
• Incident Management Services
• Problem Management Services
• Change Management Services
• Service Requests
<b>Security Services</b>
<b>Service Asset and Configuration Management</b>
<b>Siebel Services</b>
<b>Transition Services</b>

#### 6.1.3 Automated Regression Test Suite M&O:

Effective beginning August 15, 2018, Contractor shall operate, maintain, and update the Automated Regression Test Suite (ARTS) previously developed by the State's Third Party Vendor for DDI. Contractor will provide the services in accordance with the terms below from one of its hosted environments. State will also operate, maintain and update the ARTS in the State's Citrix environment. The ARTS tool validates application functionalities and sub-system connectivity of VHC using presently 61 test cases scripted and developed using the Hewlett Packard (HP) Unified Functional Tool (UFT).

##### 6.1.3.1 Contractor shall perform the following activities pertaining to the operation of the ARTS:

- a. Contractor shall schedule and run the ARTS script once per month in Contractor's environment;
- b. In the event of test case failures, Contractor shall, upon State's request, execute up to 4 additional ARTS script runs within the 30-day period following the initial test case failures; in no event shall the script be run more than once per week;
- c. Contractor shall monitor and confirm test case success or failure
- d. Contractor shall verify that the UFT is sending email notifications of test case results to State distribution list;

- e. Contractor shall triage all test case failures and work with State to identify necessary remediation;
- f. Contractor shall remediate test case failures up to the Non-Discretionary Service Request threshold hours, unless otherwise agreed to by the parties;
- g. Contractor shall provide reasonable consultation to help address questions about the tool; and
- h. Contractor shall, upon request, assist State's efforts to set up, schedule, review result reports, and analyze test script failures in connection with State's monthly Citrix environment ARTS script execution; provided that State maintains currency with all HP UFT and ARTS updates as provided by Contractor.

6.1.3.2 Contractor shall perform the following activities pertaining to the maintenance of the ARTS:

- a. Contractor shall maintain existing ARTS and test cases, including M&O VHC application patching, Medicaid Federal Poverty Level (FPL), and other reasonable maintenance required to keep test cases up to date. For those test cases that require updating due to Contractor's M&O releases, Contractor shall maintain these test cases up to 20 hours of combined development and unit testing per release, up to five times per Contract year. In the event more hours for development and/or unit testing is required for these test cases, Contractor and State will determine if additional support will be as provided under Section 6.1.3.3(a) or continue to be supported under this provision;
- b. Contractor shall maintain the existing ARTS custom Graphical User Interface (GUI) applet;

6.1.3.3 Contractor shall perform the following activities pertaining to updating the ARTS:

- a. Contractor shall update existing regression suite test cases totaling up to 80 hours of combined development and Unit testing per release up to four times per Contract year;
- b. Contractor shall develop up to two new test cases per year up to a total of 200 hours per Contract Year and based on mutually agreed prioritization;
- c. In order to make updated versions of the HP UFT software available to State, Contractor shall update in its own environment its instance of the HP UFT software as updates and upgrades become available (to the extent necessary to maintain currency within two releases of the most recent version or as agreed to by both parties), and shall provide up to 20 hours of combined development and unit testing per update for redesign of the test case(s) that may be necessary due to their lack of compatibility with the new HP UFT version;
- d. Contractor shall notify the State regarding any ARTS updates in Contractor's hosted environment through existing OCRB process;
- e. Contractor shall track all updates to the ARTS via the Apache Subversion (SVN) version control system; including datasheets and expected results;
- f. Contractor shall provision State users to ARTS update information in SVN;
- g. Validation of test case changes will be done during the next scheduled execution of the suite;
- h. Updates that exceed Contractor's expected 80 hours of combined development and Unit Testing or exceed Contractor's expected development for new test cases may be subject to the Change Request process;

- i. Contractor shall coordinate ARTS update schedules with State;
- j. In order to maintain currency with updates and versions of the ARTS in Citrix environment, Contractor shall allow State up to 14 calendar days for installation from the date upon which script updates are reviewed by both parties

6.1.3.4 Contractor shall not be obligated to perform the following tasks and activities, which Contractor and State acknowledge and agree are outside of the scope of services to be provided under Section 6.1.3:

- a. Enhancements of the ARTS beyond test case updates and development of additional test cases as described in 6.1.3.3 above;
- b. Combined development and unit testing services for redesign of the test case(s) in excess of 20 hours relating to a particular HP UFT Software updates or upgrades per Section 6.1.3.3 (c) ;
- c. All support of the State's Citrix server (e.g. User provisioning, migration of tool to another server, maintenance of UFT, and triage or maintenance of Citrix server), except as stated in Section 6.1.3.1(h) provided State maintains currency as stated in Section 6.1.3.3(j) with the most recent ARTS updates deployed through the release management process;
- d. Remediation of UFT defects due to either State patching of its Citrix server or State's UFT upgrades on its Citrix server;
- e. Any training of State users for the ARTS;
- f. Changes to original ARTS documents provided by the State's Third Party Vendor for DDI other than as necessary to reflect test case updates made by Contractor pursuant to Sections 6.1.3.2 and 6.1.3.3.

### **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 a "# Recon: 834 Transaction Removal," however, Contractor will also be subject to certain Service Level terms and conditions set forth in Exhibit 2 to this Attachment A. RSRs other than "# Recon: 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.

### **6.3 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: (1) the Deliverable Identifier (“Req”) Number, (2) Key Deliverable Designation (Yes/No); (3) the Requirement Name, (4) the DED Submission Timeframe; (5) the 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	Yes	Project Management Plan	3 Weeks after Effective Date	4 Weeks after DED Approval	Annually
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	Quarterly
1.K04	Yes	M&O Schedule	3 weeks after Effective Date	4 Weeks after DED Approval	Monthly
1.K05	Yes	Architecture Document	6 weeks after Effective Date	4 Weeks after DED Approval	every 6 months
1.K06	Yes	Availability Plan	6 weeks after Effective Date	4 Weeks after DED Approval	Quarterly
1.K07	Yes	Configuration Management Plan	9 weeks after Effective Date	4 Weeks after DED Approval	Quarterly
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	Quarterly
2.N03	No	Capacity Plan	9 weeks after Effective Date	4 Weeks after DED Approval	Every Six Months
2.N04	No	Event Management Plan	9 weeks after Effective Date	4 Weeks after DED Approval	Quarterly
2.N05	No	Source Code Management Plan	16 weeks after Effective Date	5 Weeks after DED Approval	Every Six Months
2.N06	No	System Performance and Reliability Plan	16 weeks after Effective Date	5 Weeks after DED Approval	Quarterly
2.N07	No	Defect Management Plan	12 weeks after Effective Date	5 Weeks after DED Approval	Quarterly
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	Every Six Months

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 12: DED Review and Approval Process; and Attachment A, Section 14: Deliverables Review and Approval Process.
- Notwithstanding the DED Submission Timeframe set forth above, in the event the Contractor 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 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 Deliverable Expectation Document (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) Project Management Plan (PMP)**

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

##### **(2) 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.
- ix. One failover table top 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.

### **(3) M&O Manual**

Contractor shall develop for the State's review and Acceptance, an M&O Manual that are 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;
- vi. Provisioning and de-provisioning users.

**(4) 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.

**(5) 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.

**(6) 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;
- vii. Process for opening RFCs will follow the State's existing Change Management documentation, if monitoring/Incidents require change to Service/CI.

**(7) 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 Configuration Management Database (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;
- viii. Strategy for providing State reporting (and raw data upon request) based upon KPIs, metrics outlined within these NFRs.

#### **(8) 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.

#### **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."

#### **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 and that are to be submitted in accordance to the project schedule, but these do not require Acceptance by the State. Reports are tied to Core M&O Services and are found in Table B.

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	Operational Business Report	10th business day of the month, starting the second month of the Contract
2.D03	Capacity Reporting	10th business day of the month, starting the second month of the Contract
2.D04	Change Management Reporting	10th business day of the month, starting the second month of the Contract
2.D05	Configuration Reporting	10th business day of the month, starting the second month of the Contract
2.D06	Event Reporting	10th business day of the month, starting the second month of the Contract
2.D07	Incident Management Report	10th business day of the month, starting the second month of the Contract
2.D08	Managed Application Version Reporting	10th business day of the month, starting the second month of the Contract and quarterly thereafter
2.D09	Problem Management Reporting	10th business day of the month, starting the second month of the Contract, and weekly thereafter
2.D10	Release 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	Change Requests Log	10th business day of the month, starting the second month of the Contract
2.D19	Risk Log	10th business day of the month, starting the second month of the Contract and weekly thereafter
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 which 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

### **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. Specification of the characteristics of the physical and/or virtual server on which 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.
  - d. 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 C 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.
- 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.
- 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.
- 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 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. 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;

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

## 9. 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;

- 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.
  - 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.
  - 3. Represent M&O criteria and its impact on the HSEP platform on behalf of State at the OCRB.

## 10. 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.

## **11. 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 12 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 12 below.

## **12. 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) 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) 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) day period, the State has neither accepted, nor provided comments on the DED, the DED may be escalated pursuant to Section 17 in Attachment A.

## **13. 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 DED. If the State fails to provide approval of the DED, the Contractor and State shall endeavor to resolve any remaining issues within one (1) business day.

#### **14. 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) 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) 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) day period, the State has neither accepted, nor provided comments on the Deliverable, the Deliverable may be escalated pursuant to Section 17 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.

#### **15. 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.

#### **16. OPERATIONAL CHANGE REQUEST PROCESS**

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.

## **17. INFORMAL DISPUTE RESOLUTION PROCESS**

The parties desire that all disputes arising under this Contract be resolved expeditiously, amicable, 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.

## **18. 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.
- (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.

## 19. 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.

## 20. 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.

**Automated Regression Test Suite (ARTS)** means a tool that validates application functionalities and sub-system connectivity of VHC using test cases scripted and developed using the Hewlett Packard Unified Functional Tool (UFT).

**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, other Third Party Vendors.

**Discretionary Service Request** 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 16 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.

**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.

**ODU** means Oracle Unified Directory.

**OVD** means Oracle Virtual Directory.

**Party** or **Parties** shall 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, 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.



## **21. 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.

## **22. 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.

This cooperation effort shall occur when State is going through software license certification efforts and/or audits from software vendors. The State has budgeted for a third-party provider to assist with certification. 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.

## **23. 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.

## **24. 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 16 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 includes \$1,500,000.00 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.

**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	<b>1.000</b>	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	<b>1.001</b>	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	<b>1.002</b>	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	<b>1.003</b>	Evaluate, identify and recommend changes to enhance performance of the Managed Applications.
Application Maintenance and Operation Services	Application Maintenance Tuning	<b>1.004</b>	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	<b>1.005</b>	Provide data backup and recovery for data which is less than 4 days old and available within RMAN.
Application Maintenance and Operation Services	Configuration Management	<b>1.006</b>	Perform configuration management for components of all Managed Applications, which entails the identification, control, maintenance and verification of configuration items, and the maintenance of the configuration management database and report on configuration changes.

Functional Area	Sub Area	Req. #	Requirement
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 in to 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.
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.

Functional Area	Sub Area	Req. #	Requirement
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 Operation Services	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 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.

Functional Area	Sub Area	Req. #	Requirement
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.
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.

Functional Area	Sub Area	Req. #	Requirement
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.
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.



Functional Area	Sub Area	Req. #	Requirement
Application Maintenance and Operation Services	Production Schedule Services	<b>1.040</b>	Prepare batch jobs for execution for Production and Non-production environments.
Application Maintenance and Operation Services	Production Schedule Services	<b>1.041</b>	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	<b>1.042</b>	Provide quality control for reprocessing activities, such as batch reruns.
Application Maintenance and Operation Services	Release Services	<b>1.043</b>	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.
Application Maintenance and Operation Services	Release Services	<b>1.044</b>	Plan and oversee the roll-out of Minor Releases of Managed Applications, including break-fix and Non-Discretionary Service Requests.
Availability Management	General Requirements	<b>1.045</b>	Investigate and remediate Incidents and Problems which impact Availability within the scope of the Contractor's responsibilities under this Contract.
Availability Management	General Requirements	<b>2.000</b>	The Availability Plan shall be reviewed and updated quarterly.
Availability Management	General Requirements	<b>2.001</b>	Contractor shall execute all activities within the Availability Plan.
Availability Management	General Requirements	<b>2.002</b>	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	<b>2.003</b>	Document and publish the availability of the critical and high priority services that apply to the Contractor's Core M&O Services.

Functional Area	Sub Area	Req. #	Requirement
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.
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.

Functional Area	Sub Area	Req. #	Requirement
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.
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.

Functional Area	Sub Area	Req. #	Requirement
Disaster Recovery Services	General Requirements	<b>5.000</b>	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	<b>5.001</b>	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	<b>5.002</b>	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 readily accessible in the event Contractor and/or State are unable to gain normal access.
Disaster Recovery Services	General Requirements	<b>5.003</b>	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	<b>5.004</b>	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.
Disaster Recovery Services	General Requirements	<b>5.005</b>	The Contractor shall provide evidence to State quarterly -- through logs, reporting and service reviews -- that its Service Continuity plan is integrated with the HSEP Change and Configuration Management expectations and processes.
Disaster Recovery Services	General Requirements	<b>5.006</b>	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	<b>5.007</b>	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.

Functional Area	Sub Area	Req. #	Requirement
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.
Disaster Recovery Services	General Requirements	5.009	Contractor shall provide its Business Continuity Plan for the M&O Services that they provide (e.g. Command Center, ITSM System, and Application Support). The process shall be reviewed by the State and the Contractor shall continually improve and link to Organizational and Operational Change Management.
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.

Functional Area	Sub Area	Req. #	Requirement
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: <ul style="list-style-type: none"> <li>• Manage and monitor SLAs including availability, reliability, throughput, and capacity.</li> <li>• Perform logging and Monitoring of ECM Infrastructure.</li> <li>• Maintain the service composites.</li> <li>• Perform runtime Service Usage Tracking, Monitoring, Alert Notifications, and Exception Management.</li> <li>• Maintain Federal Cloud connectivity.</li> </ul>
Enterprise Content Management Services	General Requirements	6.010	Error Logs for WC maintained and reviewed and reviewed on a daily recurring frequency.

Functional Area	Sub Area	Req. #	Requirement
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.
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: <ul style="list-style-type: none"> <li>• Tools utilized</li> <li>• Monitoring location(s)</li> <li>• Synthetic transactions utilized</li> <li>• Calculations used to determine thresholds, alerts, baselines and service reports.</li> </ul>
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, OEM)



Functional Area	Sub Area	Req. #	Requirement
Event Management/ Monitoring	General Requirements	<b>8.010</b>	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	<b>8.011</b>	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	<b>8.012</b>	Contractor will monitor the Services by utilizing the tools, methods and approach specified in the Event Management Plan.
Event Management/ Monitoring	General Requirements	<b>8.013</b>	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	<b>8.014</b>	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	<b>8.015</b>	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 tools 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: <ul style="list-style-type: none"> <li>• 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.</li> <li>• Monitor events in OIM for issues related to user registration and provisioning.</li> </ul> Runtime Service Usage Tracking, Monitoring, Alert Notifications, and Exception Management.
Identity & Access Management Services	General Requirements	9.005	Performance: <ul style="list-style-type: none"> <li>• Meet business performance requirements of throughput and capacity.</li> <li>• Conduct regular capacity planning of the IAM components in all environments and adjust infrastructure sizing as needed</li> <li>• Confirm IAM components remain integrated with Managed Applications during normal operations and upgrades (excludes major upgrades which shall be handled by DDI).</li> </ul>

Functional Area	Sub Area	Req. #	Requirement
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.
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.

Functional Area	Sub Area	Req. #	Requirement
Knowledge Management	General Requirements	10.001	Define workflow, including editing, review and approvals for creation of knowledge artifacts.
MDM & Access Integration Services	General Requirements	11.000	Contractor shall perform those services, functions and responsibilities identified with respect to the installation, configuration and management of the MDM & Non-State Access Integration infrastructure components and their related interfaces which will enable the exchange of information both within the internal systems and with external partners.
MDM & Access Integration Services	General Requirements	11.001	Confirm proper operation of the MDM and non-State Access Integration infrastructure.
MDM & Access Integration Services	General Requirements	11.002	Manage and monitor availability, reliability, and performance of MDM and non-State Access Integration components to meet the expectations of the solution.
MDM & Access Integration Services	General Requirements	11.003	Maintain MDM and non-State Access Integration related software currency at Contractor recommended patch levels.
MDM & Access Integration Services	General Requirements	11.004	Manage Environment instance configurations with internal and external partners.
MDM & Access Integration Services	General Requirements	11.005	Maintain the existing MDM and Access Integration related AIA/PIP composites including management of their source code, version control and deployment.
MDM & Access Integration Services	General Requirements	11.006	Confirm proper backups of all environments are being taken and perform MDM and/or non-State Access Integration system recovery if needed.
MDM & Access Integration Services	General Requirements	11.007	Confirm necessary application configurations are maintained to prevent any interruptions in interface transmissions and allow continued connectivity for HSEP and Access integration functionality for all integrated environments.
MDM & Access Integration Services	General Requirements	11.008	Perform controlled stops and restarts to MDM and non-State Access Integration servers as needed.
MDM & Access Integration Services	General Requirements	11.009	Participate in data governance activities and assist State personnel with same.
MDM & Access Integration Services	General Requirements	11.010	Troubleshoot and resolve issues within the scope of this Contract that arise within the interfaces to and from MDM and the Access Integration related software components.

Functional Area	Sub Area	Req. #	Requirement
MDM & Access Integration Services	General Requirements	<b>11.011</b>	The Contractor shall support the usage, monitoring, troubleshooting, and performance of the MDM and Access Integration infrastructure.
MDM & Access Integration Services	General Requirements	<b>11.012</b>	The Contractor shall participate in any required governance and change management processes.
MDM & Access Integration Services	General Requirements	<b>11.013</b>	Provide, install, configure, and maintain the MDM and non-State Access Integration components (Siebel UCM, OEDQ, Oracle DB, Oracle Client, Oracle HTTPS Web Server, Java, Tomcat Application Server, SFTP, custom code and scripts).
MDM & Access Integration Services	General Requirements	<b>11.014</b>	Conduct regular capacity planning of the MDM and non-State Access Integration related components in all environments and adjust infrastructure sizing as needed.
MDM & Access Integration Services	General Requirements	<b>11.015</b>	Manage and enforce policies for authentication, encryption, and decryption of the MDM and Access Integration interface data. Audit data fields as required.
MDM & Access Integration Services	General Requirements	<b>11.016</b>	Contractor will manage MDM application performance to meet the expectations of the HSEP.
Release Management	General Requirements	<b>12.000</b>	Each pre-production release shall include the following: <ul style="list-style-type: none"> <li>• Release-specific hardware and Managed Application components.</li> <li>• 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.</li> <li>• Detailed configuration information for any 3rd party hardware and software. Vendor shall provide updated documentation when upgrades to software or equipment occurs.</li> </ul>
Release Management	General Requirements	<b>12.001</b>	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	<b>12.002</b>	Contractor shall provide access for appropriate and authorized State team members to the test and training environments to confirm correct implementation of changes

Functional Area	Sub Area	Req. #	Requirement
			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.
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.

Functional Area	Sub Area	Req. #	Requirement
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: <ul style="list-style-type: none"> <li>• Integration plan with other processes (Incident, Problem, Release, Configuration)</li> <li>• Responsibility matrix (RACI)</li> <li>• 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</li> <li>• 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</li> <li>• Maintain transparency for all Changes in the system of record with State and other parties as directed by State.</li> </ul>
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.
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.



Functional Area	Sub Area	Req. #	Requirement
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.
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.

Functional Area	Sub Area	Req. #	Requirement
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.
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.

Functional Area	Sub Area	Req. #	Requirement
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.
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.

Functional Area	Sub Area	Req. #	Requirement
Request Services	Incident Management Services	<b>13.027</b>	State has ultimate authority for determining ticket impact, urgency and priority in accordance with the criteria identified in Attachment A, Section 6.1.1 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	<b>13.028</b>	Classify the Incident according to Priority Level with the State having final approval for that priority level.
Request Services	Incident Management Services	<b>13.029</b>	Investigate and diagnose the Incident.
Request Services	Incident Management Services	<b>13.030</b>	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	<b>13.031</b>	Following an Incident's restoration, State shall close the Ticket upon State approval.
Request Services	Incident Management Services	<b>13.032</b>	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	<b>13.033</b>	Follow agreed upon procedures maintained by the State for Security Incidents.
Request Services	Incident Management Services	<b>13.034</b>	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	<b>13.035</b>	Escalate Incidents in accordance with mutually agreed upon Contractor's procedures.

Functional Area	Sub Area	Req. #	Requirement
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.
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.

Functional Area	Sub Area	Req. #	Requirement
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: <ul style="list-style-type: none"> <li>• Incident, Problem and Change Management, inclusive of the following:</li> <li>• Change Requests/Orders originating from CCB</li> <li>• Changes reviewed and approved at OCRB</li> <li>• Request Fulfillment</li> </ul>
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 (ITSM) Services	13.049	Contractor shall provide encryption via HTTPS / TLS for access to the ITSM System.
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.



Functional Area	Sub Area	Req. #	Requirement
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.
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.

Functional Area	Sub Area	Req. #	Requirement
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 20, Defined Terms 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.



Functional Area	Sub Area	Req. #	Requirement
Request Services	Problem Management Services	<b>13.076</b>	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	<b>13.077</b>	Escalate Problem investigation in accordance with mutually agreed upon Contractor's procedures.
Request Services	Problem Management Services	<b>13.078</b>	Update Problem Tickets in the Ticket Management System to reflect current status.
Request Services	Problem Management Services	<b>13.079</b>	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	<b>13.080</b>	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	<b>13.081</b>	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	<b>13.082</b>	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	<b>13.083</b>	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	<b>13.084</b>	Provide the Service Desk Services in English.
Request Services	Service Desk Support	<b>13.085</b>	Escalate issues related to the Managed Applications that are not within Contractor's Scope of responsibility.
Request Services	Service Desk Support	<b>13.086</b>	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	<b>13.087</b>	The ITSM system shall act as the central repository and single source of truth for ticketing data, information and reporting.

Functional Area	Sub Area	Req. #	Requirement
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.
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.
Request Services	Service Requests	13.096	Develop test plans, as appropriate, for Minor Releases and Service Requests and provide such test plans to State.
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.

Functional Area	Sub Area	Req. #	Requirement
Request Services	Service Requests	<b>13.100</b>	Comply with the QA procedures and relevant application quality and security standards.
Request Services	Service Requests	<b>13.101</b>	Maintain a Request Fulfillment process (a.k.a. non-discretionary work order process) based upon State's existing process.
Request Services	Service Requests	<b>13.102</b>	Provide workflow for submission, tracking, updating, and managing Service Requests.
Request Services	Service Requests	<b>13.103</b>	Participate as reasonably requested by State in State's requirements definition and prioritization activities.
Request Services	Service Requests	<b>13.104</b>	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	<b>13.105</b>	Migrate code throughout appropriate environments and incorporate changes into production code baseline.
Security Services	General Requirements	<b>14.000</b>	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	<b>14.001</b>	Contractor shall participate in yearly risk assessments used to identify risks to the HSEP platform.
Security Services	General Requirements	<b>14.002</b>	Contractor shall participate in Incident response training, tabletop, and testing events as required by Contract.
Security Services	General Requirements	<b>14.003</b>	Contractor shall participate in periodic updates to privacy impact assessment documentation.
Security Services	General Requirements	<b>14.004</b>	Provide bi-annual entitlement review reports for State attestations and perform remediation of over provisioned or inappropriate access.
Security Services	General Requirements	<b>14.005</b>	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.

Functional Area	Sub Area	Req. #	Requirement
Security Services	General Requirements	<b>14.006</b>	Responsible for technical code and application configuration remediation activities for ongoing outstanding security weaknesses (identified via audits and POAM findings).
Security Services	General Requirements	<b>14.007</b>	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	<b>14.008</b>	Contractor will assist with maintaining current inventory documentation that includes: Database, Web, Infrastructure and application components.
Security Services	General Requirements	<b>14.009</b>	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: <ul style="list-style-type: none"> <li>• Brief description of the Incident</li> <li>• Incident category (lost stolen, unauthorized access, etc.)</li> <li>• Type of device involved</li> <li>• Suspected PII Breach</li> </ul>
Security Services	General Requirements	<b>14.010</b>	Upon request, Contractor will provide artifacts for State to maintain and update required security and compliance documents including: <ul style="list-style-type: none"> <li>• State Security Plan</li> <li>• Plan of Action and Milestones</li> <li>• IRS Corrective Action Plans</li> </ul>
Security Services	General Requirements	<b>14.011</b>	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	<b>14.012</b>	The Contractor shall confirm proper security and compliance for Managed Applications as established in Exhibit 3.
Security Services	General Requirements	<b>14.013</b>	Comply with applicable Security Policies in Exhibit 3 including CMS policies and the State of Vermont policies, adopted by the State Department of Information and Innovation, 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

Functional Area	Sub Area	Req. #	Requirement
			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	Compliant 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: <ul style="list-style-type: none"> <li>• Provide notification of confirmed or unsuccessful Notification Events impacting Contractor-provided or Managed Applications and HSEP databases</li> <li>• Technical remediation of application configuration or code elements that have identified security flaws as a result of events under the scope of this Contract</li> <li>• Report a Notification Event so the State may appropriately inform regulatory agency</li> </ul>
Security Services	General Requirements	14.017	Contractor will adhere to secure coding practices and State required secure SDLC process, which entails the following: <ul style="list-style-type: none"> <li>• Contractor will perform secure code scanning through a service provided by the State</li> <li>• Remediation of findings with code produced</li> <li>• Submission of code and secure development scanning leveraging State provided static and dynamic code review tools</li> <li>• Participate in security impact analysis for all sensitive code promoted to production</li> <li>• Documentation of results and dispositions for code remediated</li> </ul>
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.

Functional Area	Sub Area	Req. #	Requirement
Security Services	General Requirements	14.021	Security: <ul style="list-style-type: none"> <li>• Manage and enforce policies for authentication, encryption, and decryption.</li> <li>• Perform WebCenter user and role management including Federal Cloud access and State internal access.</li> <li>• Install, configure, and support one-way and two-way certificate based authentication.</li> </ul>
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	Compliant 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 Configuration Management	General Requirements	15.001	Contractor shall execute applicable activities within the Service Asset and Configuration processes.
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.



Functional Area	Sub Area	Req. #	Requirement
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.
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.

Functional Area	Sub Area	Req. #	Requirement
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.
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 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
Siebel Services	General Requirements	16.002	Perform routine configuration resource maintenance of the middleware to support middleware changes and changes in the hosting Environments.
Siebel Services	General Requirements	16.003	Provide maintenance and support for middleware and supporting utilities and perform middleware system recovery.
Siebel Services	General Requirements	16.004	Perform controlled stops and restarts to middleware servers as needed.



Functional Area	Sub Area	Req. #	Requirement
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: <ul style="list-style-type: none"> <li>• Unit &amp; System test Siebel Objects</li> <li>• Conflict resolution (merge vs. over-write) of imported objects</li> <li>• Deployment across environments</li> </ul>
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: <ul style="list-style-type: none"> <li>• Install/Configure and maintain following server applications <ul style="list-style-type: none"> <li>-Gateway</li> <li>-Siebel server</li> <li>-Database server</li> <li>-Web servers</li> <li>-BI Publisher</li> </ul> </li> <li>• Configure and maintain the following: <ul style="list-style-type: none"> <li>-Communication Server SMTP/POP3</li> <li>-Workflow Monitor Agents</li> <li>-Email Manager Communication templates for workflow</li> <li>-Workflow Policies and Actions</li> </ul> </li> </ul>
Siebel Services	General Requirements	16.008	Maintain the Siebel environments through the performance of the following activities: <ul style="list-style-type: none"> <li>• Code migration from Development to Production (across all environments).</li> <li>Siebel Remote (as needed).</li> <li>Siebel Anywhere to push out .srf and .rox.</li> <li>Handle issues with Transaction Processor, Merger and Router.</li> <li>Disaster recovery.</li> <li>Support issues with HI States.</li> <li>Support and apply Java upgrades.</li> <li>Siebel High Interactive (HI).</li> <li>Resolve software issues on desktop impacts Siebel HI State.</li> <li>• Maintain/support the organizational access structure for State employees in Siebel: <ul style="list-style-type: none"> <li>Organizations.</li> <li>Divisions.</li> <li>Positions.</li> <li>Responsibilities.</li> <li>Views.</li> <li>Users/Employees.</li> </ul> </li> </ul>

Functional Area	Sub Area	Req. #	Requirement
Siebel Services	General Requirements	<b>16.009</b>	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	<b>16.010</b>	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	<b>17.000</b>	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	<b>17.001</b>	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.

## 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 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 (Excluded 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 20 of Attachment A:

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

1	System Availability .....	75
2	System Incident Notification and Restoration.....	81
3	Root Cause Analysis/Debrief .....	83
4	Representative Transaction Performance Measures.....	84
5	Disaster Recovery (DR) .....	86
6	Plan of Action and Milestones (POA&M) Remediation Requirements and Credits .....	87
7	Reconciliation Service Requests .....	88
8	Service Level Credits Methodology .....	91

### 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
- Downtime Minutes

EXAMPLE:

- Example 1

Siebel Primary Business Component in Production is down for 20 minutes on October 7<sup>th</sup> and 35 minutes on October 20<sup>th</sup>. During the October 20<sup>th</sup> 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:

$$\begin{aligned} \text{Downtime minutes} &= 20 + (35 - 15) = 40 \text{ minutes} \\ \text{Availability percentage} &= (44,640 - 40 \text{ downtime minutes}) / 44,640 \times 100 = 99.91\% \end{aligned}$$

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 7<sup>th</sup> and 30 minutes on October 20<sup>th</sup>. The Availability percentage is computed as follows:

$$\begin{aligned} \text{Downtime minutes} &= 25 + 30 = 55 \text{ minutes} \\ \text{Availability percentage} &= (44,640 - 55 \text{ downtime minutes}) / 44,640 \times 100 = 99.87\% \end{aligned}$$

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 10<sup>th</sup> business day of the month following the reporting month. For example, July’s report will be due by August 12<sup>th</sup>. 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.	Earn Back Credit During non-Open Enrollment period.
		Then the Earn Back Credit equals the	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:	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 Earnback 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 is a report of all Priority level 1, Priority level 2 incidents that occurred during the month with their response, notification, and resolution times.

Once an incident has been established as either Priority level 1 or Priority level 2, the Contractor shall notify the State within fifteen (15) minutes for Priority 1 and within one (1) hour for Priority 2 of this designation. 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.

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.

2.1 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.

The time frame begins immediately upon the Contractor becoming aware of the P1 or a P2 Incident via the Contractor's Ticketing System. Start time will be taken from the timestamp of the first update made by the Contractor resource within the ticketing system. 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 weeks of the occurrence.

## 2.2 Definitions

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, the actual work needs to be implemented via the agreed upon change management process.

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 Start Time: The maximum amount of time from when an issue is established as an incident that the Contractor shall start working on a resolution for that incident.

Restoration Time: The maximum amount of time from when an issue is established as an incident to when there that incident has a resolution.

Initial Notification: The maximum amount of time from when an issue is established as an incident to 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
<b>Level 1 Incidents (P1)</b>	Within 15 minutes	4 hours	Within 15 minutes	Every 1 hours	Daily at the end of each business day	Reported monthly in System Availability reports.
<b>Level 2 Incidents (P2)</b>	Within one hour	8 hours	Within 60 minutes	Every 1 hours	Daily at the end of each business day	Reported monthly in System Availability reports.

### 2.3 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.

Contractor shall deliver the report to the AHS IT Manager, DVHA Operations Director, and upload it into the “knowledge repository” no later than the 10<sup>th</sup> 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 12<sup>th</sup>.

Service Level Credit	<p>0.25% reduction of the monthly fee for Core M&amp;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.</p> <p>0.5% reduction of the monthly fee for Core M&amp;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</p>
----------------------	---

2.4 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
- Probable root cause of the incident

Root Cause Analysis (RCA) status (validated, still under investigation, fixed)

- 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)
- 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 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 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 10<sup>th</sup> 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 12<sup>th</sup>.

##### 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 Windows
- (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
- (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 <b>2.0 seconds</b>

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% 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.

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 of up to the 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](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.

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. POAM 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 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
<p>Upon the Identification Date of a weakness against Controls, Contractor and State will initiate the Commencement phase.</p> <p>Initiate Commencement Phase - the following 3 steps must occur within 30 calendar days unless excused performance or otherwise agreed to by the parties:</p> <p>(1) State and Contractor meet to validate identified weakness and determine ownership;</p> <p>(2) Contractor will draft and submit plans of action milestones, target completion dates for each milestone, and resources required;</p> <p>(3) The State will confirm acceptance of contractor POA&amp;M data submission(s), providing risk ranking changes (if necessary) and initiate entry to State POA&amp;M;</p>	<p>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&amp;M as appropriate until Remediation Date.</p>	<p>Data sources used in assessments against the Controls include the following:</p> <ul style="list-style-type: none"> <li>• independent assessments</li> <li>• self-attestations</li> <li>• vulnerability assessments</li> <li>• pen test or</li> <li>• incident/risk reports</li> </ul>	<p>Contractor shall Remediate the severity of risk as follows unless as otherwise agreed to by both parties:</p> <p>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).</p> <p>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).</p> <p>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).</p>

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

7.1 Contractor will use reasonable, good-faith efforts to address State's Reconciliation Service Requests (RSRs) without unreasonable delay. Effective as of August 15, 2018, with respect only to



the specific type of RSR referred to by State and Contractor as a “# Recon: 834 Transaction Removal”, Contractor will also be subject to the Service Level terms and conditions set forth in Sections 7 and 8 of this Service Level Agreement. Contractor shall prioritize “# Recon: 834 Transaction Removal” RSRs between a Priority 2 Incident and a Priority 3 Incident. Contractor will complete “# Recon: 834 Transaction Removal” RSRs in accordance with Table F below, subject to the maximum allowable per day or per month, as set forth in Table F. “# Recon: 834 Transaction Removal” RSRs in excess of such daily or monthly limits will not be subject to any Service Level Metric triggering a Service Level Credit and will be addressed with reasonable and good-faith efforts in the ordinary course.

Contractor’s Service Level obligations under this Section 7 with respect to any RSR are conditioned on State’s submission of the RSR through the ITSM system, including its identification as a “# Recon: 834 Transaction Removal” RSR in the Short Description field in the ITSM system when applicable. Table F provides the number of maximum daily and monthly “# Recon: 834 Transaction Removal” RSR requests that are subject to Service Level Metrics, and related Service Level Credits, if any.

## 7.2 Definitions

The column headers in Table F have the following meanings:

Reconciliation Type Description: The type of RSR addressed by the Contractor that is subject to this SLA.

Maximum Number of RSRs Applicable to Service Level Metrics per Day: The maximum number of “# Recon: 834 Transaction Removal” RSRs submitted per day for which the Service Level Metric will be applicable.

Maximum Number of RSRs Applicable to Service Level Metrics per Month: The maximum number of “# Recon: 834 Transaction Removal” RSRs submitted per month to which the Service Level Metric will be applicable.

Service Level Metric: The maximum amount of time from when the “# Recon: 834 Transaction Removal” RSR is submitted to the Contractor until the ITSM ticket is placed in a “Resolved” status.

# Recon: 834 Transaction Removal: Removal of an 834 transaction Case from the 834 batch prior to that batch being sent to the carrier; also referred to as a BGN pull.

**Table F: Reconciliation Service Requests Applicable to Service Level Metrics**

Reconciliation Type Description	Maximum Number of RSRs Applicable to Service Level Metrics per Day	Maximum Number of RSRs Applicable to Service Level Metrics per Month	Service Level Metric
# Recon: 834 Transaction Removal	10	20	Contractor shall remove 834 transaction prior to the next scheduled 834 batch transmission*

\*Applicable only to those Recon: 834 Transaction Removal requests received from State at least 60 minutes prior to a scheduled 834 batch transmission. Further, in the event of a P1/P2 incident that directly impedes the Contractor's ability to use the system to complete a "# Recon: 834 Transaction Removal" RSR, the time during which the P1/P2 Incident occurred will not be counted towards the Service Level Metric measurement time.

### 7.3 Measurement Tracking

The measurement starts when the incident ticket is created by State in ITSM and assigned to the Contractor and ends when the ticket is updated with a "Resolved" status by Contractor. If a "# Recon: 834 Transaction Removal" is in a "Resolved" status prior to the next scheduled 834 batch transmission the SLA shall be deemed presumptively met. The State reserves the right to re-evaluate presumptively resolved tickets upon reasonable cause. Notwithstanding the foregoing, any amount of time a RSR ticket spends in "Waiting Client" and/or "Waiting IT" status in the ITSM, it shall not be included in the Service Level measurement.

### 7.4 Reporting

Contractor shall report RSRs submitted by State through the ITSM system monthly to the State. The report will detail all RSRs for the month by ITSM identification number, description, open date/time, target complete date/time, actual complete date/time, and SLA status.

Contractor shall include "# Recon: 834 Transaction Removal" RSR measurement as part of the Service Level Report to the AHS IT Manager, DVHA Operations Director, and upload it into the "knowledge repository" no later than the 10<sup>th</sup> business day of the month following the reporting month. For example, the July 2016 report will be due by August 12<sup>th</sup>. 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 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 "# Recon: 834 Transaction Removal" RSR that did not meet the Service Level Metric in Table F, with a maximum of up to the At-Risk Amount.
----------------------	--

### 7.5 Out of Scope

The following RSRs will not be subject to any Service Level Metric or Service Level Credit:

- i. Any RSRs other than “# Recon: 834 Transaction Removal” RSRs
- ii. Any “# Recon: 834 Transaction Removal” RSRs in excess of the daily or monthly thresholds as defined in this Section.
- iii. Any “# Recon: 834 Transaction Removal” RSRs with respect to which Contractor’s ability to meet its Service Level Metric was materially impaired by defects caused by a recent VHC Production Release.
- iv. Any “# Recon: 834 Transaction Removal” RSRs with respect to which Contractor’s ability to meet its Service Level Metric was materially impaired by defects in a third-party system.

## **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 10% percent 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 Department of Information and Innovation, 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. Compliant 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 (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, (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 the contract year commencing August 15, 2018:

- IRS Office of Safeguards Audit September 2018
- Independent Assessment Audit of the 3 sites containing live data for the Authority to Connect (ATC), on a date to be determined by the parties.
- Self-Attestation due June, 2019.

#### **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 14.

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
- 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.

## 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:

Susan Whitney, Grants and Contracts Administrator  
Business Office, Contracting Unit  
Department of Vermont Health Access  
NOB 1 South, 280 State Drive  
Waterbury, VT 05671-1010
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
Discretionary Services Amount	\$ 1,500,000.00
Key Deliverables*	\$ 3,300,000.00
Total	\$37,114,250.00

\*The total fee for Key Deliverables is comprised of the \$2,200,000.00 outlined in Table A and the \$1,100,000.00 outlined in Table A1 in this Attachment B.

#### 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 1/24<sup>th</sup> 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.

#### 9.2 Discretionary Services

Additional services not explicitly described in Attachment A, but which are approved by a Change Request as referenced in Sections 16 and 24 of Attachment A, include a Not To Exceed (NTE) amount for all such Discretionary Services of \$1,500,000.00.

### 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 and (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 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	\$150,000.00	\$12,500.00
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. It is understood and agreed that:

- Where applicable, the content of all Deliverables delineated in Table A and Table A1 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 12, 13 and 14: 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 Contractor 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 11 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 A1 of this Attachment B which are estimated dates and may be updated as agreed upon via the M&O Schedule.

**10. Additional Fulfiller Licenses.** Fulfiller Licenses may be purchased in blocks of ten (10) at a total cost for such block of licenses of \$6,000.

**ATTACHMENT C: STANDARD STATE PROVISIONS  
FOR CONTRACTS AND GRANTS  
REVISED DECEMBER 15, 2017**

**1. Definitions:** For purposes of this Attachment, “Party” shall mean the Contractor, Grantee or Subrecipient, with whom the State of Vermont is executing this Agreement and consistent with the form of the Agreement. “Agreement” shall mean the specific contract or grant to which this form is attached.

**2. Entire Agreement:** This Agreement, whether in the form of a contract, State-funded grant, or Federally-funded grant, represents the entire agreement between the parties on the subject matter. All prior agreements, representations, statements, negotiations, and understandings shall have no effect.

**3. Governing Law, Jurisdiction and Venue; No Waiver of Jury Trial:** This Agreement will be governed by the laws of the State of Vermont. Any action or proceeding brought by either the State or the Party in connection with this Agreement shall be brought and enforced in the Superior Court of the State of Vermont, Civil Division, Washington Unit. The Party irrevocably submits to the jurisdiction of this court for any action or proceeding regarding this Agreement. The Party agrees that it must first exhaust any applicable administrative remedies with respect to any cause of action that it may have against the State with regard to its performance under this Agreement. Party agrees that the State shall not be required to submit to binding arbitration or waive its right to a jury trial.

**4. Sovereign Immunity:** The State reserves all immunities, defenses, rights or actions arising out of the State’s sovereign status or under the Eleventh Amendment to the United States Constitution. No waiver of the State’s immunities, defenses, rights or actions shall be implied or otherwise deemed to exist by reason of the State’s entry into this Agreement.

**5. No Employee Benefits For Party:** The Party understands that the State will not provide any individual retirement benefits, group life insurance, group health and dental insurance, vacation or sick leave, workers compensation or other benefits or services available to State employees, nor will the State withhold any state or Federal taxes except as required under applicable tax laws, which shall be determined in advance of execution of the Agreement. The Party understands that all tax returns required by the Internal Revenue Code and the State of Vermont, including but not limited to income, withholding, sales and use, and rooms and meals, must be filed by the Party, and information as to Agreement income will be provided by the State of Vermont to the Internal Revenue Service and the Vermont Department of Taxes.

**6. Independence:** The Party will act in an independent capacity and not as officers or employees of the State.

**7. Defense and Indemnity:** The Party shall defend the State and its officers and employees against all third party claims or suits arising in whole or in part from any act or omission of the Party or of any agent of the Party in connection with the performance of this Agreement. The State shall notify the Party in the event of any such claim or suit, and the Party shall immediately retain counsel and otherwise provide a complete defense against the entire claim or suit. The State retains the right to participate at its own expense in the defense of any claim. The State shall have the right to approve all proposed settlements of such claims or suits.

After a final judgment or settlement, the Party may request recoupment of specific defense costs and may file suit in Washington Superior Court requesting recoupment. The Party shall be entitled to recoup costs only upon a showing that such costs were entirely unrelated to the defense of any claim arising from an act or omission of the Party in connection with the performance of this Agreement.

The Party shall indemnify the State and its officers and employees if the State, its officers or employees become legally obligated to pay any damages or losses arising from any act or omission of the Party or an agent of the Party in connection with the performance of this Agreement.

Notwithstanding any contrary language anywhere, in no event shall the terms of this Agreement or any document furnished by the Party in connection with its performance under this Agreement obligate the State to (1) defend or

indemnify the Party or any third party, or (2) otherwise be liable for the expenses or reimbursement, including attorneys' fees, collection costs or other costs of the Party or any third party.

**8. Insurance:** Before commencing work on this Agreement the Party must provide certificates of insurance to show that the following minimum coverages are in effect. It is the responsibility of the Party to maintain current certificates of insurance on file with the State through the term of this Agreement. No warranty is made that the coverages and limits listed herein are adequate to cover and protect the interests of the Party for the Party's operations. These are solely minimums that have been established to protect the interests of the State.

*Workers Compensation:* With respect to all operations performed, the Party shall carry workers' compensation insurance in accordance with the laws of the State of Vermont. Vermont will accept an out-of-state employer's workers' compensation coverage while operating in Vermont provided that the insurance carrier is licensed to write insurance in Vermont and an amendatory endorsement is added to the policy adding Vermont for coverage purposes. Otherwise, the party shall secure a Vermont workers' compensation policy, if necessary to comply with Vermont law.

*General Liability and Property Damage:* With respect to all operations performed under this Agreement, the Party shall carry general liability insurance having all major divisions of coverage including, but not limited to:

Premises - Operations

Products and Completed Operations

Personal Injury Liability

Contractual Liability

The policy shall be on an occurrence form and limits shall not be less than:

\$1,000,000 Each Occurrence

\$2,000,000 General Aggregate

\$1,000,000 Products/Completed Operations Aggregate

\$1,000,000 Personal & Advertising Injury

*Automotive Liability:* The Party shall carry automotive liability insurance covering all motor vehicles, including hired and non-owned coverage, used in connection with the Agreement. Limits of coverage shall not be less than \$500,000 combined single limit. If performance of this Agreement involves construction, or the transport of persons or hazardous materials, limits of coverage shall not be less than \$1,000,000 combined single limit.

*Additional Insured.* The General Liability and Property Damage coverages required for performance of this Agreement shall include the State of Vermont and its agencies, departments, officers and employees as Additional Insureds. If performance of this Agreement involves construction, or the transport of persons or hazardous materials, then the required Automotive Liability coverage shall include the State of Vermont and its agencies, departments, officers and employees as Additional Insureds. Coverage shall be primary and non-contributory with any other insurance and self-insurance.

*Notice of Cancellation or Change.* There shall be no cancellation, change, potential exhaustion of aggregate limits or non-renewal of insurance coverage(s) without thirty (30) days written prior written notice to the State.

**9. Reliance by the State on Representations:** All payments by the State under this Agreement will be made in reliance upon the accuracy of all representations made by the Party in accordance with this Agreement, including but not limited to bills, invoices, progress reports and other proofs of work.

**10. False Claims Act:** The Party acknowledges that it is subject to the Vermont False Claims Act as set forth in 32 V.S.A. § 630 *et seq.* If the Party violates the Vermont False Claims Act it shall be liable to the State for civil penalties, treble damages and the costs of the investigation and prosecution of such violation, including attorney's fees, except as the same may be reduced by a court of competent jurisdiction. The Party's liability to the State under the False Claims Act shall not be limited notwithstanding any agreement of the State to otherwise limit Party's liability.

**11. Whistleblower Protections:** The Party shall not discriminate or retaliate against one of its employees or agents for disclosing information concerning a violation of law, fraud, waste, abuse of authority or acts threatening health or safety, including but not limited to allegations concerning the False Claims Act. Further, the Party shall not require such employees or agents to forego monetary awards as a result of such disclosures, nor should they be required to report misconduct to the Party or its agents prior to reporting to any governmental entity and/or the public.

**12. Location of State Data:** No State data received, obtained, or generated by the Party in connection with performance under this Agreement shall be processed, transmitted, stored, or transferred by any means outside the continental United States, except with the express written permission of the State.

**13. Records Available for Audit:** The Party shall maintain all records pertaining to performance under this agreement. "Records" means any written or recorded information, regardless of physical form or characteristics, which is produced or acquired by the Party in the performance of this agreement. Records produced or acquired in a machine readable electronic format shall be maintained in that format. The records described shall be made available at reasonable times during the period of the Agreement and for three years thereafter or for any period required by law for inspection by any authorized representatives of the State or Federal Government. If any litigation, claim, or audit is started before the expiration of the three-year period, the records shall be retained until all litigation, claims or audit findings involving the records have been resolved.

**14. Fair Employment Practices and Americans with Disabilities Act:** Party agrees to comply with the requirement of 21 V.S.A. Chapter 5, Subchapter 6, relating to fair employment practices, to the full extent applicable. Party shall also ensure, to the full extent required by the Americans with Disabilities Act of 1990, as amended, that qualified individuals with disabilities receive equitable access to the services, programs, and activities provided by the Party under this Agreement.

**15. Set Off:** The State may set off any sums which the Party owes the State against any sums due the Party under this Agreement; provided, however, that any set off of amounts due the State of Vermont as taxes shall be in accordance with the procedures more specifically provided hereinafter.

**16. Taxes Due to the State:**

- A. Party understands and acknowledges responsibility, if applicable, for compliance with State tax laws, including income tax withholding for employees performing services within the State, payment of use tax on property used within the State, corporate and/or personal income tax on income earned within the State.
- B. Party certifies under the pains and penalties of perjury that, as of the date this Agreement is signed, the Party 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.
- C. Party understands that final payment under this Agreement may be withheld if the Commissioner of Taxes determines that the Party is not in good standing with respect to or in full compliance with a plan to pay any and all taxes due to the State of Vermont.
- D. Party also understands the State may set off taxes (and related penalties, interest and fees) due to the State of Vermont, but only if the Party has failed to make an appeal within the time allowed by law, or an appeal has been taken and finally determined and the Party has no further legal recourse to contest the amounts due.

**17. Taxation of Purchases:** All State purchases must be invoiced tax free. An exemption certificate will be furnished upon request with respect to otherwise taxable items.

**18. Child Support:** (Only applicable if the Party is a natural person, not a corporation or partnership.) Party states that, as of the date this Agreement is signed, he/she:

- A. is not under any obligation to pay child support; or
- B. is under such an obligation and is in good standing with respect to that obligation; or
- C. has agreed to a payment plan with the Vermont Office of Child Support Services and is in full compliance with that plan.

Party makes this statement with regard to support owed to any and all children residing in Vermont. In addition, if the Party is a resident of Vermont, Party makes this statement with regard to support owed to any and all children residing in any other state or territory of the United States.

**19. Sub-Agreements:** Party shall not assign, subcontract or subgrant the performance of this Agreement or any portion thereof to any other Party without the prior written approval of the State. Party shall be responsible and liable to the State for all acts or omissions of subcontractors and any other person performing work under this Agreement pursuant to an agreement with Party or any subcontractor.

In the case this Agreement is a contract with a total cost in excess of \$250,000, the Party shall provide to the State a list of all proposed subcontractors and subcontractors' subcontractors, together with the identity of those subcontractors' workers compensation insurance providers, and additional required or requested information, as applicable, in accordance with Section 32 of The Vermont Recovery and Reinvestment Act of 2009 (Act No. 54).

Party shall include the following provisions of this Attachment C in all subcontracts for work performed solely for the State of Vermont and subcontracts for work performed in the State of Vermont: Section 10 ("False Claims Act"); Section 11 ("Whistleblower Protections"); Section 12 ("Location of State Data"); Section 14 ("Fair Employment Practices and Americans with Disabilities Act"); Section 16 ("Taxes Due the State"); Section 18 ("Child Support"); Section 20 ("No Gifts or Gratuities"); Section 22 ("Certification Regarding Debarment"); Section 30 ("State Facilities"); and Section 32.A ("Certification Regarding Use of State Funds").

**20. No Gifts or Gratuities:** Party shall not give title or possession of anything of substantial value (including property, currency, travel and/or education programs) to any officer or employee of the State during the term of this Agreement.

**21. Copies:** Party shall use reasonable best efforts to ensure that all written reports prepared under this Agreement are printed using both sides of the paper.

**22. Certification Regarding Debarment:** Party certifies under pains and penalties of perjury that, as of the date that this Agreement is signed, neither Party nor Party'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.

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

**23. Conflict of Interest:** Party shall fully disclose, in writing, any conflicts of interest or potential conflicts of interest.

**24. Confidentiality:** Party acknowledges and agrees that this Agreement and any and all information obtained by the State from the Party in connection with this Agreement are subject to the State of Vermont Access to Public Records Act, 1 V.S.A. § 315 et seq.

**25. Force Majeure:** Neither the State nor the Party shall be liable to the other for any failure or delay of performance of any obligations under this Agreement to the extent such failure or delay shall have been wholly or principally caused by acts or events beyond its reasonable control rendering performance illegal or impossible (excluding strikes or lock-outs) ("Force Majeure"). Where Force Majeure is asserted, the nonperforming party must prove that it made all reasonable efforts to remove, eliminate or minimize such cause of delay or damages, diligently pursued



performance of its obligations under this Agreement, substantially fulfilled all non-excused obligations, and timely notified the other party of the likelihood or actual occurrence of an event described in this paragraph.

**26. Marketing:** Party shall not refer to the State in any publicity materials, information pamphlets, press releases, research reports, advertising, sales promotions, trade shows, or marketing materials or similar communications to third parties except with the prior written consent of the State.

**27. Termination:**

- A. Non-Appropriation:** If this Agreement extends into more than one fiscal year of the State (July 1 to June 30), and if appropriations are insufficient to support this Agreement, the State may cancel at the end of the fiscal year, or otherwise upon the expiration of existing appropriation authority. In the case that this Agreement is a Grant that is funded in whole or in part by Federal funds, and in the event Federal funds become unavailable or reduced, the State may suspend or cancel this Grant immediately, and the State shall have no obligation to pay Subrecipient from State revenues.
- B. Termination for Cause:** Either party may terminate this Agreement if a party materially breaches its obligations under this Agreement, and such breach is not cured within thirty (30) days after delivery of the non-breaching party's notice or such longer time as the non-breaching party may specify in the notice.
- C. Termination Assistance:** Upon nearing the end of the final term or termination of this Agreement, without respect to cause, the Party shall take all reasonable and prudent measures to facilitate any transition required by the State. All State property, tangible and intangible, shall be returned to the State upon demand at no additional cost to the State in a format acceptable to the State.

**28. Continuity of Performance:** In the event of a dispute between the Party and the State, each party will continue to perform its obligations under this Agreement during the resolution of the dispute until this Agreement is terminated in accordance with its terms.

**29. No Implied Waiver of Remedies:** Either party's delay or failure to exercise any right, power or remedy under this Agreement shall not impair any such right, power or remedy, or be construed as a waiver of any such right, power or remedy. All waivers must be in writing.

**30. State Facilities:** If the State makes space available to the Party in any State facility during the term of this Agreement for purposes of the Party's performance under this Agreement, the Party shall only use the space in accordance with all policies and procedures governing access to and use of State facilities which shall be made available upon request. State facilities will be made available to Party on an "AS IS, WHERE IS" basis, with no warranties whatsoever.

**31. Requirements Pertaining Only to Federal Grants and Subrecipient Agreements:** If this Agreement is a grant that is funded in whole or in part by Federal funds:

- A. Requirement to Have a Single Audit:** The Subrecipient will complete the Subrecipient Annual Report annually within 45 days after its fiscal year end, informing the State of Vermont whether or not a Single Audit is required for the prior fiscal year. If a Single Audit is required, the Subrecipient will submit a copy of the audit report to the granting Party within 9 months. If a single audit is not required, only the Subrecipient Annual Report is required.

For fiscal years ending before December 25, 2015, a Single Audit is required if the subrecipient expends \$500,000 or more in Federal assistance during its fiscal year and must be conducted in accordance with OMB Circular A-133. For fiscal years ending on or after December 25, 2015, a Single Audit is required if the subrecipient expends \$750,000 or more in Federal assistance during its fiscal year and must be conducted in accordance with 2 CFR Chapter I, Chapter II, Part 200, Subpart F. The Subrecipient Annual Report is required to be submitted within 45 days, whether or not a Single Audit is required.

- B. Internal Controls:** In accordance with 2 CFR Part II, §200.303, the Party must establish and maintain effective internal control over the Federal award to provide reasonable assurance that the Party is managing the Federal award in compliance with Federal statutes, regulations, and the terms and conditions of the award. These internal controls should be in compliance with guidance in “Standards for Internal Control in the Federal Government” issued by the Comptroller General of the United States and the “Internal Control Integrated Framework”, issued by the Committee of Sponsoring Organizations of the Treadway Commission (COSO).
- C. Mandatory Disclosures:** In accordance with 2 CFR Part II, §200.113, Party must disclose, in a timely manner, in writing to the State, all violations of Federal criminal law involving fraud, bribery, or gratuity violations potentially affecting the Federal award. Failure to make required disclosures may result in the imposition of sanctions which may include disallowance of costs incurred, withholding of payments, termination of the Agreement, suspension/debarment, etc.

**32. Requirements Pertaining Only to State-Funded Grants:**

- A. Certification Regarding Use of State Funds:** If Party is an employer and this Agreement is a State-funded grant in excess of \$1,001, Party certifies that none of these State funds will be used to interfere with or restrain the exercise of Party’s employee’s rights with respect to unionization.
- B. Good Standing Certification (Act 154 of 2016):** If this Agreement is a State-funded grant, Party hereby represents: (i) that it has signed and provided to the State the form prescribed by the Secretary of Administration for purposes of certifying that it is in good standing (as provided in Section 13(a)(2) of Act 154) with the Agency of Natural Resources and the Agency of Agriculture, Food and Markets, or otherwise explaining the circumstances surrounding the inability to so certify, and (ii) that it will comply with the requirements stated therein.

(End of Standard Provisions)

**ATTACHMENT D  
OTHER TERMS AND CONDITIONS**

1. Section 2, "Entire Agreement" of Attachment C is hereby modified to add the following sentence at the end:

In the event that one or more provisions of this Contract are found to be invalid, unenforceable or illegal by a Court of competent jurisdiction, the remaining terms shall remain in full force and effect.

2. The second sentence of Section 27.A "Non-Appropriation" of Attachment C, is deleted in its entirety and replaced with the following:

In the case that this Contract is funded in whole or in part by federal or other non-State funds, and in the event those funds become unavailable or reduced, the State agrees to give notice to the Party within two business days after a non-funding event. This Contract shall immediately terminate upon the Party's receipt of this notice and the State shall make payments for Core M&O Services rendered and M&O Deliverables accepted prior to the notification of the non-funding event.

3. Section 27.B "Termination for Cause" of Attachment C, is modified to add the following at the end:

For avoidance of doubt, Contractor may terminate in the event State fails to pay undisputed Contractor Charges when due and thereafter fails to make such payment within thirty days after receipt of written notice from Contractor that Contractor intends to terminate for such failure to pay.

4. (a) The first paragraph of Section 7, "Defense and Indemnity" of Attachment C is hereby deleted in its entirety and replaced with the following:

The Party shall defend the State and its officers and employees against all third-party claims or suits arising in whole or in part from any act or omission of the Party or of any agent of the Party in connection with the performance of this Agreement. The State shall notify the Party in the event of any such claim or suit, and the Party shall immediately retain counsel and otherwise provide a complete defense against the entire claim or suit. The State retains the right to participate at its own expense in the defense of any claim. The State shall have the right to approve all proposed settlements of such claims or suits. In the event the State withholds approval to settle any such claim, then the Party shall proceed with the defense of the claim but under those circumstances, the Party's indemnification obligations shall be limited to the amount of the proposed settlement initially rejected by the State.

- (b) The last paragraph of Section 7, "Defense and Indemnity" of Attachment C is hereby deleted in its entirety and replaced with the following:

Notwithstanding any contrary language anywhere, in no event shall the terms of this Contract or any document furnished by the Party in connection with its performance under this Contract obligate the State to (1) defend or indemnify the Party, or (2) otherwise be liable for the expenses or reimbursement, including attorneys' fees, collection costs or other costs of the Party. This statement does not waive or preclude any independent remedies that would exist under law. The Party shall not be responsible for the indemnity of the State to the extent damages or losses arise

from the acts or omissions of the State, its officers or employees, including the State's unauthorized or illegal use of or modification to the deliverables under this Contract.

5. Section 31, "Requirements Pertaining to Federal Grants and Subrecipient Agreements" of Attachment C is hereby modified by the addition of the following:

To the extent Contractor determines itself to be a "subrecipient", Contractor shall comply with A, B and C as listed herein.

6. Section 13, "Records Available for Audit" of Attachment C is hereby deleted in whole and replaced with the following:

**Records Available for Audit.** The Contractor shall maintain records pertaining solely to Contractor's performance under this agreement, limited to verifying accuracy of Contractor's charges and invoices and verifying Contractor's performance of the Services as agreed upon by the parties in Attachment A of this Contract. "Records" means any written or recorded information, regardless of physical form or characteristics, which is produced or acquired by the Contractor in the performance of this Contract. Records produced or acquired in a machine readable electronic format shall be maintained in that format. The records described shall be made available at reasonable times provided there is prior notice to the Contractor during the period of the Contract and for three years thereafter or for any period required by law for inspection by any authorized representatives of the State or Federal Government. If any litigation, claim, or audit is started before the expiration of the three year period, the records shall be retained until all litigation, claims or audit findings involving the records have been resolved.

7. Section 19, "Sub-Agreements" of Attachment C is hereby modified to add the following sentence at the end:

Notwithstanding the foregoing, Contractor may utilize staff-augmentation contractors or staff from affiliates in the ordinary course of business, and in every such instance, prior written approval of the State shall not be required. Contractor shall be responsible for liability arising from the acts or omissions of such contractors, affiliates and other agents, including any worker's compensation liability or unemployment insurance liability for which the State may otherwise be determined by the State of Vermont Department of Labor to be liable.

8. Section 12, "Location of State Data" of Attachment C is hereby amended to add the following sentence at the end:

Notwithstanding the foregoing, the State consents to Contractors use of off-shore resources to support non-production data.

## **9. ORDER OF PRECEDENCE; CONTRACTOR DOCUMENTATION**

The parties specifically agree that any language or provisions contained in a Contractor Document is of no force and effect if such language or provisions conflict with the terms of Attachment C or Attachment D to this Contract. Further, in no event shall any Contractor Document: (a) require indemnification by

the State of the Contractor; (b) waive the State's right to a jury trial; (c) establish jurisdiction in any venue other than the Superior Court of the State of Vermont, Civil Division, Washington Unit; (d) designate a governing law other than the laws of the State of Vermont; (e) constitute an implied or deemed waiver of the immunities, defenses, rights or actions arising out of State's sovereign status or under the Eleventh Amendment to the United States Constitution; or (f) limit the time within which an action may be brought hereunder.

For purposes of this Attachment D, "Contractor Document" shall mean one or more document, agreement or other instrument required by the Contractor in connection with the performance of the services set forth in Attachment A hereto, regardless of format, and any other paper or "shrinkwrap," "clickwrap," or other electronic version thereof.

## 10. TERM OF CONTRACTOR'S DOCUMENTS

Contractor acknowledges and agrees that, to the extent a Contractor Document provides for alternate term or termination provisions, including automatic renewals, such sections shall be waived and shall have no force and effect. All Contractor Documents shall run concurrently with **the term of this Contract; provided, however, to the extent the State has purchased a perpetual** license to use the Contractor's or Contractor's third party software, hardware or other services, such license shall remain in place unless expressly terminated in accordance with the terms of this Contract.

## 11. OWNERSHIP AND LICENSE IN DELIVERABLES

**11.1 Contractor Intellectual Property.** Contractor shall retain all right, title and interest in and to all Contractor Intellectual Property that Contractor delivers to the State in accordance with Attachment A of this Contract. "**Contractor Intellectual Property**" means any work, ideas, inventions, discoveries, tools, methodology, compute programs, processes and improvements, computer processes, specifications, operating instructions, notes and any other documentation (whether or not patentable) that (a) has been created by Contractor or its third party supplier prior to entering into this Contract, (b) will be created during the Term of this Contract or thereafter but outside the scope of this Contract and (c) customizations or modifications to tangible or intangible property falling within the definitions of (a) or (b) even if created as a provision of the Services set forth in this Contract by either Contractor or a third party supplier or subcontractor. Contractor or Contractor's third party supplier or subcontractor shall retain ownership of any and all Contractor Intellectual Property, provided that if any Intellectual Property is included as part of a Work Product or is otherwise delivered to the State under this Contract, such Contractor Intellectual Property shall be licensed to the State and CMS on a non-exclusive basis for the State to use in connection with the Work Product or if a stand-alone deliverable, then in accordance with the Contractor or applicable third party's standard end user license agreement, with rights no less restrictive than that set forth in 45 C.F.R. 74.36 and 45 C.F.R. 92.34.

State hereby grants to Contractor an irrevocable, royalty-free perpetual, world-wide license to use, have used, improve, further develop and sub-license intangible Work Product developed under this Contract for any public sector business purpose. Further, State hereby grants to Contractor a license to use, have used, improve, further develop and sub-license intangible Work Product developed under this Contract for any commercial business purpose on such terms as the

parties may agree. State may copyright any work that is subject to copyright and was developed, or for which ownership was purchased, under this Contract.

Contractor shall report to the State, promptly and in written detail, any notice or claim of copyright infringement received by Contractor with respect to all deliverables and Work Product under this Contract.

To the extent Contractor delivers any intangible property developed with private funding or otherwise developed outside the scope of this Contract, the State will have Restricted Rights (1) if such property is non-commercial software; (2) the Contractor's standard commercial license, if such property is commercial software; and (3) limited rights, if such property is other than software. Restricted Rights means that the software may not be used, reproduced, or disclosed except that it may be: (1) used or copied for use with the computer(s) for which it was acquired; (2) used or copied for use with a backup computer if any computer for which it was acquired is inoperative; (3) reproduced for safekeeping (archives) or backup purposes; (4) modified, adapted, or combined with other computer software, provided that the modified, adapted, or combined portions of the derivative software incorporating any of the delivered, restricted computer software shall be subject to the same restricted rights; (5) disclosed to and reproduced for use by support service contractors or their subcontractors for one of the purposes described in (1) through (4), provided that the State provides prior notice to Contractor and obtains a non-disclosure agreement with the recipients; and (6) used or copied for use with a replacement computer.

Limited Rights means that the property may be reproduced and used by the State with the express limitation that they will not, without the written permission of Contractor, be used for purposes of manufacture nor disclosed outside the State government.

When feasible, Contractor shall affix an appropriate legend to intangible property delivered under the Contract to reflect whether it is (1) developed under this contract with State or federal funds, entitling the State to a license for State purposes; (2) developed outside this contract or with private funds, and subject to Restricted Rights or Limited Rights; or (3) commercial software subject to the terms of a commercial software license.

In performing the Services, Contractor will use its proprietary intangible property, including tools and information that it will not deliver under this Contract. The State obtains no rights in any intangible property that is not a deliverable under this Contract.

To the extent that the Contractor delivers or has delivered any commercial computer software under this Contract which shall require the agreement of the State to commercial license rights in order to use the software, whether through a license agreement, end user agreement or similar agreement delivered as shrink wrap, browse-wrap or a click-through, the Contractor shall make such terms available to the State and provide full contact information of the software licensors to State upon request.

Contractor shall be utilizing the HP ALM Tool (the "HP System"). In connection with the Contractor's use of the HP System, the State acknowledges that the Contractor shall have the nonexclusive right and license to use the HP System (a) during the Term of this Contract, and (b) in conjunction with the other products and services provided by Contractor under this

Contract. Contractor's use of the HP System is subject to user limitations that may restrict the number of authorized concurrent users.

Without limiting any rights of the State in this Contract, Contractor acknowledges that this Contract is in support of the State's implementation of the Patient Protection and Affordable Care Act of 2010, and 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. This Contract is subject to, and incorporates by reference, 45 CFR 74.36 and 45 CFR 92.34 governing rights to intangible property. Contractor must deliver all Work Product to the State in a manner that ensures the Centers for Medicare & Medicaid Services, an agency of the Department of Health and Human Services, obtain a royalty-free, nonexclusive and irrevocable right to reproduce, publish or otherwise use the Work Product for Federal purposes and to authorize others to do so. "Federal purposes" include the purpose of administering health insurance exchanges under the Affordable Care Act of 2010. Contractor is further subject to applicable regulations governing patents and inventions, including those issued by the Department of Commerce at 37 CFR Part 401.

**11.2 State Intellectual Property.** The State shall retain all right, title and interest in and to all (i) State Data provided by the State, and to all information that is created under this Contract, including, but not limited to, all data that is generated under this Contract as a result of the use by Contractor, the State or any third party of any technology systems or knowledge bases that are developed for the State and used by Contractor hereunder, and all other rights, tangible or intangible and (ii) State trademarks, trade names, logos and other State identifiers, Internet uniform resource locators, State user name or names, Internet addresses and e-mail addresses obtained or developed pursuant to this Contract (collectively, "**State Intellectual Property**").

As between the State and Contractor, the State shall be deemed to own all Customer Data, and Contractor shall at all times process the Customer Data in accordance with the terms of this Contract, and all applicable Laws.

Contractor may not use State Intellectual Property for any purpose other than as required for services relating to VHC or HSE or as specified elsewhere in this Contract. Contractor acquires no rights or licenses, including, without limitation, intellectual property rights or licenses, to use State Intellectual Property for its own purposes. In no event shall the Contractor claim any security interest in State Intellectual Property.

**11.3 Work Product.** Except with respect to Contractor Intellectual Property, all Work Product shall belong exclusively to the State, with the State having the sole and exclusive right to apply for, obtain, register, hold and renew, in its own name and/or for its own benefit, all patents and copyrights, and all applications and registrations, renewals and continuations thereof and/or any and all other appropriate protection. To the extent exclusive title and/or complete and exclusive ownership rights in and to any Work Product may not originally vest in the State by operation of law or otherwise as contemplated hereunder, Contractor shall immediately upon request, unconditionally and irrevocably assign, transfer and convey to the State all right, title and interest therein. For the avoidance of doubt, Work Product shall not be deemed to include Contractor Intellectual Property, provided the State shall be granted an irrevocable, perpetual, non-exclusive royalty-free license to any such Contractor Intellectual Property that is

incorporated into Work Product, provided that nothing in this paragraph shall reduce or otherwise diminish Contractor's right to use the Work Product as set forth herein.

## **12. CONFIDENTIALITY AND NON-DISCLOSURE; SECURITY BREACH REPORTING**

**12.1 Confidentiality of Contractor Information.** The Contractor acknowledges and agrees that this Contract and any and all Contractor information obtained by the State in connection with this Contract are subject to the State of Vermont Access to Public Records Act, 1 V.S.A. § 315 et seq. The State will not disclose information for which a reasonable claim of exemption can be made pursuant to 1 V.S.A. § 317(c), including, but not limited to, trade secrets, proprietary information or financial information, including any formulae, plan, pattern, process, tool, mechanism, compound, procedure, production data, or compilation of information which is not patented, which is known only to the Contractor, and which gives the Contractor an opportunity to obtain business advantage over competitors who do not know it or use it.

The State shall immediately notify Contractor of any request made under the Access to Public Records Act, or any request or demand by any court, governmental agency or other person asserting a demand or request for Contractor information. Contractor may, in its discretion, seek an appropriate protective order, or otherwise defend any right it may have to maintain the confidentiality of such information under applicable State law within three business days of the State's receipt of any such request. Contractor agrees that it will not make any claim against the State if the State makes available to the public any information in accordance with the Access to Public Records Act or in response to a binding order from a court or governmental body or agency compelling its production. Contractor shall indemnify the State for any costs or expenses incurred by the State, including, but not limited to, attorneys' fees awarded in accordance with 1 V.S.A. § 320, in connection with any action brought in connection with Contractor's attempts to prevent or unreasonably delay public disclosure of Contractor's information if a final decision of a court of competent jurisdiction determines that the State improperly withheld such information and that the improper withholding was based on Contractor's attempts to prevent public disclosure of Contractor's information.

The State agrees that (a) it will use the Contractor information only as may be necessary in the course of performing duties, receiving services or exercising rights under this Contract; (b) it will provide at a minimum the same care to avoid disclosure or unauthorized use of Contractor information as it provides to protect its own similar confidential and proprietary information; (c) except as required by the Access to Records Act, it will not disclose such information orally or in writing to any third party unless that third party is subject to a written confidentiality agreement that contains restrictions and safeguards at least as restrictive as those contained in this Contract; (d) it will take all reasonable precautions to protect the Contractor's information; and (e) it will not otherwise appropriate such information to its own use or to the use of any other person or entity.

Contractor may affix an appropriate legend to Contractor information that is provided under this Contract to reflect the Contractor's determination that any such information is a trade secret, proprietary information or financial information at time of delivery or disclosure.



**12.2 Confidentiality of State Information.** In performance of this Contract, and any exhibit or schedule hereunder, the Party acknowledges that certain State Data (as defined below), to which the Contractor may have access may contain individual federal tax information, personal protected health information and other individually identifiable information protected by State or federal law. In addition to the provisions of this Section, the Party shall execute the Business Partner Agreement attached as Attachment E. Before receiving or controlling State Data, the Contractor will have an information security policy that protects its systems and processes and media that may contain State Data from internal and external security threats and State Data from unauthorized disclosure, and will have provided a copy of such policy to the State. State Data that is personally identifiable information as defined in 9 V.S.A. 2430, "Protected Health Information" as defined under 45 CFR 160.103, Federal Tax Information as defined by IRS Publication 1075 and any other State information which may be exempt from disclosure under 3 V.S.A 317 (together, "State Data") shall not be stored, accessed from, or transferred to any location outside the United States. Notwithstanding the foregoing, it is understood Contractor, or its affiliates or agents performing services hereunder outside of the United States, will have access to passwords, access codes, user identifications, security procedures or similar information to perform services under the Contract.

Unless otherwise instructed by the State, Contractor agrees to keep confidential all State Data received and collected by Contractor in connection with this Contract. The Contractor agrees not to publish, reproduce, or otherwise divulge any State Data in whole or in part, in any manner or form or authorize or permit others to do so. Contractor will take reasonable measures as are necessary to restrict access to State Data in the Contractor's possession to only those employees on its staff who must have the information on a "need to know" basis. The Contractor shall use State Data only for the purposes of and in accordance with this Contract. The Contractor shall provide at a minimum the same care to avoid disclosure or unauthorized use of State Data as it provides to protect its own similar confidential and proprietary information.

Contractor shall cause all Contractor Personnel charged with performing Services in connection with this Contract, or who are otherwise in a position to obtain or be granted access to State Information, to execute a non-disclosure agreement or the like in a form acceptable to the State. Contractor shall require that all Contractor Personnel comply with the provisions of the non-disclosure agreement and Contractor is responsible for any failure of any Contractor Personnel to comply with all such provisions.

The Contractor shall promptly notify the State of any request or demand by any court, governmental agency or other person asserting a demand or request for State Data to which the Contractor or any third party hosting service of the Contractor may have access, so that the State may seek an appropriate protective order.

### **13. SECURITY OF STATE INFORMATION.**

For purposes of the Services performed hereunder, the Contractor shall follow the existing State control framework including industry standard administrative, technical, and physical safeguards and controls consistent with current version of CMS MARS-E (version 2), current version of IRS 1075 and Federal

Information Processing Standards Publication 200 and designed to (i) ensure the security and confidentiality of State Data; (ii) protect against any anticipated security threats or hazards to the security or integrity of the State Data; and (iii) protect against unauthorized access to or use of State Data. The Contractor will utilize State technical, operational and management measures to include at a minimum: (1) multiple levels of authentication controls to permit access to State Data only to authorized individuals and controls to prevent the Contractor employees from providing State Data to unauthorized individuals who may seek to obtain this information (whether through fraudulent means or otherwise); (2) industry-standard firewall protection; (3) access State information systems through a secure encrypted network connection to State networks where provided by the State ; (4) measures to store in a secure fashion all State Data which shall include multiple levels of authentication; (5) dual control procedures, segregation of duties, and pre-employment criminal background checks for employees with responsibilities for or access to State Data; (6) measures to ensure that the State Data shall not be altered or corrupted without the prior written consent of the State; (7) measures to protect against destruction, loss or damage of State Data due to potential environmental hazards, such as fire and water damage; (8) staff training to implement the information security measures; and (9) monitoring of the security of any portions of the Contractor systems that are used in the provision of the services against intrusion on a twenty-four (24) hour a day basis. In no event shall Contractor be liable for any non-compliance related to NIST standards that arises out of products or services to the extent such products or services fall within the State's responsibility or the responsibility of a subcontractor of the State (other than Contractor under this or any other agreement with the State).

Throughout the Term, Contractor comply with all information/technology control policies and standards applicable to the security of data, including, but not limited to, the Data Security Standards, the Insurance Industry Regulations, and Exhibit 3, Security Policies to Attachment A. If, as a result of an on-site review or audit performed in accordance with this Contract, Contractor is found not to be in compliance with such policies or standards, then Contractor shall, at its expense, take appropriate steps to promptly correct such non-compliance. Failure to promptly take reasonable steps to remediate, shall be a material breach of this Contract.

Contractor shall cause its subcontractors and agents to comply with all information/technology control policies and standards applicable to the security of data, including, but not limited to, the Data Security Standards, the Insurance Industry Regulations, and Exhibit 3[Security Policies] to Attachment A, only if and to the extent the subcontractor's scope of work, as structured by Contractor, requires adherence to the foregoing. If it is unable to do so, it shall immediately notify the State and, in consultation with the State, cause such subcontractors or agents to comply with mutually acceptable security standards.

#### **14. SECURITY BREACHES; SECURITY BREACH REPORTING.**

To the extent the Contractor or its subcontractors, affiliates or agents handles, collects, stores, disseminates or otherwise deals with State Data, the Contractor acknowledges that in the performance of its obligations under this Contract, it will be a "data collector" pursuant to Chapter 62 of Title 9 of the Vermont Statutes (9 V.S.A. §2430(3)). The Contractor shall have policies and procedures in place for the effective management of Security Breaches, as defined below.

In addition to the requirements set forth in any applicable Business Partner Agreement attached to this Contract as Attachment E, in the event of any actual security breach or reasonable belief of an actual security breach the Contractor either suffers or learns of that either compromises or could compromise State Data (including, as applicable, PII, PHI or ePHI) in any format or media, whether encrypted or unencrypted (for example, but not limited to: physical trespass on a secure facility; intrusion or hacking or other brute force attack on any State environment; loss or theft of a PC, laptop, desktop, tablet, smartphone, removable data storage device or other portable device; loss or theft of printed materials; or failure of security policies) (collectively, a "Security Breach"), the Contractor shall report any information regarding the Security Breach to the State, as soon as practicable, but in no event later than ten (10) business days from the confirmation by the Contractor of the Security Breach, except to the extent such disclosure is delayed for law enforcement purposes in accordance with applicable law.

The Contractor shall report to the State: (i) the nature of the Security Breach; (ii) the State Data used or disclosed; (iii) who made the unauthorized use or received the unauthorized disclosure; (iv) what the Contractor has done or shall do to mitigate any deleterious effect of the unauthorized use or disclosure; (v) what corrective action the Contractor has taken or shall take to prevent future similar unauthorized use or disclosure and (vi) the approximate date of the Security Breach. The Contractor shall provide such other information, including a written report, as reasonably requested by the State.

The Contractor agrees to comply with all applicable laws, as such laws may be amended from time to time (including, but not limited to, Chapter 62 of Title 9 of the Vermont Statutes, HIPAA and/or HITECH and all applicable State and federal laws, rules or regulations) that require notification in the event of unauthorized release of personally-identifiable information or other event requiring notification. In the event of a Security Breach of any of the Contractor's security obligations or other event requiring notification hereunder or under applicable law ("Notification Event"), Contractor agrees to fully cooperate with the State, assume responsibility for such notice if the State determines it to be appropriate under the circumstances of any particular Security Breach and Notification Event to the extent the Security Breach and Notification Event is the responsibility of the Contractor, and assume all costs associated with a Security Breach, including but not limited to, notice, outside investigation and services (including mailing, call center, forensics, counsel and/or crisis management), and/or credit monitoring.

In addition to any other indemnification obligations in this Contract, the Contractor shall fully indemnify and save harmless the State from any costs, loss or damage to the State resulting from a Security Breach or the unauthorized disclosure of State Data by the Contractor, its officers, agents, employees, and subcontractors, subject to the limitation cap as provided in Section 19 of this Attachment D.

## **15. DESTROYED OR LOST DATA.**

Except as otherwise provided in this Contract, Contractor will not delete or destroy any State Data or media on which State Data resides without prior authorization from the State. In the event any the State Data is lost or destroyed due to any impermissible act or omission of Contractor, including any breach of the security procedures described herein or the negligence of Contractor, Contractor shall be responsible for the prompt regeneration, reconstruction or replacement of such State Data. Contractor shall prioritize this effort so that the loss of State Data will not have any adverse effect upon the Services. The State agrees to cooperate with Contractor to provide any available information, files or raw data needed for the regeneration, reconstruction or replacement of the State Data. If Contractor fails to fully regenerate, reconstruct and/or replace any lost or destroyed State Data within the time reasonably agreed by the

parties, then the State may, at the sole cost and expense of the Contractor, obtain data reconstruction services from a third party, and Contractor shall cooperate with such third party as requested by the State.

## 16. SUBCONTRACTORS

Upon State's request, Contractor shall deliver to the State copies of such subcontracts and third party contracts.

Contractor shall use good faith efforts to have all subcontracts assignable to the State or a successor identified by the State or assignable with the consent of sub-contractor. In addition, to the extent that any subcontractor will have access to State Data or otherwise have contact with State Clientele (and prior to permitting any subcontractor to access State Data), Contractor shall be responsible for ensuring that such subcontractor is fully knowledgeable about and will comply with the rules, regulations, policies and guidelines promulgated by CMS, as well as comply with all other Insurance Industry Regulations and Data Security Standards, but only if and to the extent the subcontractor's scope of work, pursuant to its subcontract, requires subcontractor access to State Data or otherwise have contact with State Clientele. Contractor will not disclose State Data to any third party, including any Contractor Affiliates, subcontractor or other entity or any Contractor Personnel, until due and proper execution of non-disclosure agreements in a form acceptable to the State. Contractor will also cause any approved Contractor subcontractor to enter into a Business Partner Subcontract in substantially the form of the Business Partner Agreement attached to this Contract as Attachment E.

Notwithstanding the foregoing, Contractor may utilize staff-augmentation contractors or staff from affiliates for temporary assignments in the ordinary course of business, and in every such instance, prior written approval of the State shall not be required; provided however, all of the other requirements herein which apply to Contractor Personnel, including background checks, security and confidentiality obligations hereunder, shall apply.

## 17. CONTRACTOR'S REPRESENTATIONS AND WARRANTIES

**17.1 General Representations and Warranties.** The Contractor represents, warrants and covenants that:

- (i) The Contractor has all requisite power and authority to execute, deliver and perform its obligations under this Contract and the execution, delivery and performance of this Contract by the Contractor has been duly authorized by the Contractor.
- (ii) There is no pending litigation, arbitrated matter or other dispute to which the Contractor is a party which, if decided unfavorably to the Contractor, would reasonably be expected to have a material adverse effect on the Contractor's ability to fulfill its obligations under this Contract.
- (iii) The Contractor will comply with all laws applicable to its performance of the services and otherwise to the Contractor in connection with its obligations under this Contract.
- (iv) The Contractor (a) owns, or has the right to use under valid and enforceable agreements, all intellectual property rights reasonably necessary for and related to delivery of the services and provision of the Deliverables as set forth in this Contract; (b) shall be responsible for and have full authority to license all proprietary and/or third party software modules, including algorithms and protocols, that Contractor incorporates into its product; and (c) none of the Deliverables or other materials or technology provided by the

- Contractor to the State will infringe upon or misappropriate the intellectual property rights of any third party.
- (v) The Contractor has adequate resources to fulfill its obligations under this Contract.
  - (vi) Neither Contractor nor Contractor's subcontractors has past state or federal violations, convictions or suspensions relating to miscoding of employees in NCCI job codes for purposes of differentiating between independent contractors and employees.

**17.2 Contractor's Performance Warranties.** Contractor represents and warrants to the State that:

- (i) All Deliverables will be free from material errors and shall perform in accordance with the specifications therefor.
- (ii) Each and all of the services shall be performed in a timely, diligent, professional and workpersonlike manner, in accordance with the highest professional or technical standards applicable to such services, by qualified persons with the technical skills, training and experience to perform such services in the planned environment. At its own expense and without limiting any other rights or remedies of the State hereunder, the Contractor shall re-perform any services that does not meet the Acceptance criteria as agreed to by the parties
- (iii) All Deliverables supplied by the Contractor to the State shall be transferred free and clear of any and all restrictions on the conditions of transfer, modification, licensing, sublicensing and free and clear of any and all lines, claims, mortgages, security interests, liabilities and encumbrances or any kind.
- (iv) Any time software is delivered to the State, whether delivered via electronic media or the internet, no portion of such software or the media upon which it is stored or delivered will have any type of software routine or other element which is designed to facilitate unauthorized access to or intrusion upon; or unrequested disabling or erasure of; or unauthorized interference with the operation of any hardware, software, data or peripheral equipment of or utilized by the State. Notwithstanding the foregoing, Contractor assumes no responsibility for the State's negligence or failure to protect data from viruses, or any unintended modification, destruction or disclosure.

LIMITATION ON DISCLAIMER. EXCEPT WITH RESPECT TO THOSE WARRANTIES EXPRESSLY SET FORTH HEREIN, CONTRACTOR HEREBY DISCLAIMS ALL OTHER EXPRESS OR IMPLIED WARRANTIES, INCLUDING, WITHOUT LIMITATION, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE.

**18. PROFESSIONAL LIABILITY AND CYBER LIABILITY INSURANCE COVERAGE**

In addition to the insurance required in Attachment C to this Contract, before commencing work on this Contract and throughout the term of this Contract, Contractor agrees to procure and maintain (a) Technology Professional Liability insurance for any and all services performed under this Contract, with minimum third party coverage of \$5,000,000 per claim, \$5,000,000 aggregate; and (b) first party Breach Notification Coverage of not less than \$4,000,000.

Before commencing work on this Contract the Contractor must provide certificates of insurance to show that the foregoing minimum coverages are in effect.

## **19. LIMITATION OF LIABILITY.**

CONTRACTOR'S AGGREGATE LIABILITY TO THE STATE OF VERMONT IN CONNECTION WITH THIS CONTRACT SHALL NOT EXCEED ONE AND A HALF TIMES THE AGGREGATE MAXIMUM CONTRACT AMOUNT. CONTRACTOR'S AGGREGATE LIABILITY TO THE STATE OF VERMONT IN CONNECTION WITH A NOTIFICATION EVENT, AS DEFINED HEREIN, SHALL NOT EXCEED FOUR (4) MILLION DOLLARS.

LIMITS OF LIABILITY FOR STATE CLAIMS WHICH MAY BE AGREED BY THE STATE SHALL NOT APPLY TO STATE CLAIMS ARISING OUT OF: (A) CONTRACTOR'S OBLIGATION TO INDEMNIFY THE STATE; (B) CONTRACTOR'S CONFIDENTIALITY OBLIGATIONS TO THE STATE OTHER THAN A NOTIFICATION EVENT; (C) PERSONAL INJURY OR DAMAGE TO REAL OR PERSONAL PROPERTY; (D) CONTRACTOR'S GROSS NEGLIGENCE, FRAUD OR INTENTIONAL MISCONDUCT; OR (E) VIOLATIONS OF THE STATE OF VERMONT FRAUDULENT CLAIMS ACT.

IN NO EVENT SHALL CONTRACTOR'S LIABILITY BE LIMITED FOR THIRD PARTY CLAIMS AGAINST THE CONTRACTOR WHICH MAY ARISE OUT OF CONTRACTOR'S ACTS OR OMISSIONS IN THE PERFORMANCE OF THIS CONTRACT.

NEITHER PARTY SHALL BE LIABLE TO THE OTHER FOR ANY INDIRECT, INCIDENTAL OR SPECIAL DAMAGES, DAMAGES WHICH ARE UNFORESEEABLE TO THE PARTIES AT THE TIME OF CONTRACTING, DAMAGES WHICH ARE NOT PROXIMATELY CAUSED BY A PARTY, SUCH AS LOSS OF ANTICIPATED BUSINESS, OR LOST PROFITS, INCOME, GOODWILL, OR REVENUE IN CONNECTION WITH OR ARISING OUT OF THE SUBJECT MATTER OF THIS CONTRACT.

The provisions of this Section shall apply notwithstanding any other provisions of this Contract or any other agreement, and shall survive the expiration or termination of this Contract.

## **20. REMEDIES FOR DEFAULT**

In the event either party is in default under this Contract, the non-defaulting party may, at its option, pursue any or all of the remedies available to it under this Contract, including termination for cause, and at law or in equity

## **21. TERMINATION**

**SURVIVAL.** ALL SECTIONS OF THIS CONTRACT RELATING TO CONFIDENTIALITY, OWNERSHIP OF INTELLECTUAL PROPERTY, INDEMNIFICATION, GOVERNING LAW AND JURISDICTION AND LIMITATIONS OF LIABILITY SHALL SURVIVE TERMINATION OR EXPIRATION OF THIS CONTRACT.

**RETURN OF PROPERTY.** UPON TERMINATION OF THIS CONTRACT FOR ANY REASON WHATSOEVER, CONTRACTOR SHALL IMMEDIATELY DELIVER TO THE STATE ALL STATE INFORMATION, STATE INTELLECTUAL PROPERTY OR STATE DATA (INCLUDING WITHOUT LIMITATION ANY DELIVERABLES FOR WHICH STATE HAS MADE PAYMENT IN

WHOLE OR IN PART) (“STATE MATERIALS”), THAT ARE IN THE POSSESSION OR UNDER THE CONTROL OF CONTRACTOR IN WHATEVER STAGE OF DEVELOPMENT AND FORM OF RECORDATION SUCH STATE PROPERTY IS EXPRESSED OR EMBODIED AT THAT TIME.

IN THE EVENT THE CONTRACTOR CEASES CONDUCTING BUSINESS IN THE NORMAL COURSE, BECOMES INSOLVENT, MAKES A GENERAL ASSIGNMENT FOR THE BENEFIT OF CREDITORS, SUFFERS OR PERMITS THE APPOINTMENT OF A RECEIVER FOR ITS BUSINESS OR ASSETS OR AVAILS ITSELF OF OR BECOMES SUBJECT TO ANY PROCEEDING UNDER THE FEDERAL BANKRUPTCY ACT OR ANY STATUTE OF ANY STATE RELATING TO INSOLVENCY OR THE PROTECTION OF RIGHTS OF CREDITORS, THE CONTRACTOR SHALL IMMEDIATELY RETURN ALL STATE MATERIALS TO STATE CONTROL; INCLUDING, BUT NOT LIMITED TO, MAKING ALL NECESSARY ACCESS TO APPLICABLE REMOTE SYSTEMS AVAILABLE TO THE STATE FOR PURPOSES OF DOWNLOADING ALL STATE MATERIALS.

CONTRACTOR SHALL REASONABLY COOPERATE WITH OTHER PARTIES IN CONNECTION WITH ALL SERVICES TO BE DELIVERED UNDER THIS CONTRACT, INCLUDING WITHOUT LIMITATION ANY SUCCESSOR PROVIDER TO WHOM STATE MATERIALS ARE TO BE TRANSFERRED IN CONNECTION WITH TERMINATION. CONTRACTOR SHALL ASSIST THE STATE IN EXPORTING AND EXTRACTING THE STATE MATERIALS, IN A FORMAT USABLE WITHOUT THE USE OF THE SERVICES AND AS AGREED TO BY STATE, AT NO ADDITIONAL COST.

## **22. DESTRUCTION OF STATE DATA**

At any time during the term of this Contract within (i) thirty days of the State’s written request or (ii) three (3) months of termination or expiration of this Contract for any reason, and in any event after the State has had an opportunity to export and recover the State Materials, Contractor shall at its own expense securely destroy and erase from all systems it directly or indirectly uses or controls all tangible or intangible forms of the State Materials, in whole or in part, and all copies thereof except such records as are required by law. The destruction of State Data and State Intellectual Property shall be performed according to National Institute of Standards and Technology (NIST) approved methods. Contractor shall certify in writing to the State that such State Data has been disposed of securely. To the extent that any applicable law prevents Contractor from destroying or erasing State Materials as set forth herein, Contractor shall retain, in its then current state, all such State Materials then within its right of control or possession in accordance with the confidentiality, security and other requirements of this Contract, and perform its obligations under this section as soon as such law no longer prevents it from doing so.

Further, upon the relocation of State Data, Contractor shall securely dispose of such copies from the former data location and certify in writing to the State that such State Data has been disposed of securely. Contractor shall comply with all reasonable directions provided by the State with respect to the disposal of State Data.

## **23. STATE FACILITIES**

During the term of this Contract, the State may make available to Contractor space in any State facility applicable to the Services, subject to the conditions that Contractor: (i) shall only use such space solely

and exclusively for and in support of the Services; (ii) shall not use State facilities to provide goods or services to or for the benefit of any third party; (iii) shall comply with the leases, security, use and rules and agreements applicable to the State facilities; (iv) shall not use State facilities for any unlawful purpose; (v) shall comply with all reasonable policies and procedures governing access to and use of State facilities that are provided to Contractor in writing; (vi) instruct Contractor personnel not to photograph or record, duplicate, disclose, transmit or communicate any State information, materials, data or other items, tangible or intangible, obtained or available as a result of permitted use of State facilities; and (vii) return such space to the State in the same condition it was in at the commencement of this Contract, ordinary wear and tear excepted. State facilities will be made available to Contractor on an "AS IS, WHERE IS" basis, with no warranties whatsoever.

## 24. AUDIT

**Audit Rights.** Contractor will provide to the State, its internal or external auditors, clients, inspectors, regulators and other designated representatives, at reasonable times and upon 30 days prior written notice (and in the case of State or federal regulators, at any time required by such regulators with notice) access to Contractor personnel and to any and all Contractor facilities or where the required information, data and records are maintained, for the purpose of performing audits and of Contractor and/or Contractor personnel and/or any or all of the records, data and information applicable solely to this Contract. Such audits, inspections and access shall be conducted to the extent permitted or required by any laws applicable to the State or Contractor, solely to (i) verify the accuracy of charges and invoices; (ii) verify the security of State Data and examine the systems that process, store, maintain, support and transmit that data; (iii) examine and verify Contractor's and/or its permitted contractors' operations and security procedures and controls; (iv) examine and verify Contractor's and/or its permitted contractors' disaster recovery planning and testing, business resumption and testing, contingency arrangements and insurance coverage; and (v) examine Contractor's and/or its permitted contractors' performance of the Services including audits of: (1) information technology systems; (2) general controls and physical and data/information security practices and procedures; (3) quality assurance process, (4) contingency and continuity planning, disaster recovery and back-up procedures for processes, resources and data; (5) Contractor's and/or its permitted contractors' costs in performing Services; and (6) compliance with the terms of this Contract and applicable laws. Contractor shall provide and cause its permitted contractors to provide full cooperation to such auditors, inspectors, regulators and representatives in connection with audit functions and with regard to examinations by regulatory authorities. Audits conducted on Contractor's premises shall be limited to Contractor's systems and data solely related to the Services performed herein; and shall not contain the confidential information of other Contractor customers or any other systems, data or information belonging or relating to any customer other than the State. Further, the State and any auditors shall make best efforts to avoid conducting audits that may cause unnecessary disruption of Contractor's operations and shall make best efforts to avoid interference with Contractor's ability to perform the Services in accordance with any Service Levels. Additionally, any external auditor retained by the State to perform any audits shall execute a non-disclosure agreement.

## 25. CONFLICTS OF INTEREST

Contractor agrees that during the term of this Contract, its performance shall be solely in the best interest of the State. Contractor will not perform services for any person or entity which has also contracted with the State of Vermont in connection with the same project, without express written consent of the State. Contractor shall fully disclose, in writing, any such conflicts of interest, including the nature and extent



of the work to be performed for any other person or entity so that the State may be fully informed prior to giving any consent. Contractor agrees that the failure to disclose any such conflicts shall be deemed an event of default under this Contract, and this Contract shall be terminable immediately.

## **26. EXPORT CONTROL; ANTI-BRIBERY.**

Neither Contractor nor any Contractor Personnel are included on any list of entities maintained and updated by the Department of Commerce, Bureau of Industry and Security to whom the export of certain types of software is prohibited by United States' Laws, as updated from time to time ("Entity List") or list of individuals maintained and updated by the Department of Commerce, Bureau of Industry and Security to whom the export of certain types of software is prohibited by United States' Laws, as updated from time to time ("Denied Persons List") and Contractor shall never involve any entity or Contractor Personnel included on any Entity List or Denied Persons List in connection with the State account or any Services. Contractor shall provide, upon State's request and at any time new Contractor Personnel are assigned to the State account, a list of such Contractor Personnel and a statement confirming that such Contractor Personnel are not included on any Entity List or Denied Persons List. Contractor additionally acknowledges certain Software and technical data to be provided in connection with Services hereunder and certain transactions contemplated in connection with this Contract may be subject to export controls under the Laws of the United States and other countries and Contractor agrees and covenants Contractor shall not export or re-export any such items or any direct product thereof or undertake any transaction in violation of any such Laws. Contractor shall be responsible for, and shall coordinate and oversee, compliance with such Laws in respect of such items exported or imported hereunder and Contractor shall include with copies of all State Software provided by State to Contractor that Contractor is permitted to use outside of the United States specific documentation stating that "These commodities, technology or software were exported from the United States in accordance with the Export Administration Regulations. Diversion or re-export contrary to U.S. law is prohibited." Contractor has not violated Laws or any policies referenced herein regarding the offering of inducements in connection with this Contract.

## **27. CONTRACTOR BANKRUPTCY.**

Contractor acknowledges that if Contractor, as a debtor in possession, or a trustee in bankruptcy in a case under Section 365(n) of Title 11, United States Code (the "Bankruptcy Code"), rejects this Contract, the State may elect to retain its rights under this Contract as provided in Section 365(n) of the Bankruptcy Code. Upon written request of the State to Contractor or the Bankruptcy Trustee, Contractor or such Bankruptcy Trustee shall not interfere with the rights of the State as provided in this Contract, including the right to obtain the State Intellectual Property.

ATTACHMENT E  
BUSINESS ASSOCIATE AGREEMENT

**THIS BUSINESS ASSOCIATE AGREEMENT (“AGREEMENT”) IS ENTERED INTO BY AND BETWEEN THE STATE OF VERMONT AGENCY OF HUMAN SERVICES, OPERATING BY AND THROUGH ITS DEPARTMENT OF VERMONT HEALTH ACCESS (“COVERED ENTITY”) AND OPTUMINSIGHT, INC. (“BUSINESS ASSOCIATE”) AS OF AUGUST 14, 2016 (“EFFECTIVE DATE”). THIS AGREEMENT SUPPLEMENTS AND IS MADE A PART OF THE CONTRACT/GRAANT TO WHICH IT IS ATTACHED.**

Covered Entity and Business Associate enter into this Agreement to comply with standards promulgated under the Health Insurance Portability and Accountability Act of 1996 (“HIPAA”), including the Standards for the Privacy of Individually Identifiable Health Information, at 45 CFR Parts 160 and 164 (“Privacy Rule”), and the Security Standards, at 45 CFR Parts 160 and 164 (“Security Rule”), as amended by Subtitle D of the Health Information Technology for Economic and Clinical Health Act (HITECH), and any associated federal rules and regulations.

The parties agree as follows:

**1. Definitions.** All capitalized terms used but not otherwise defined in this Agreement have the meanings set forth in 45 CFR Parts 160 and 164 as amended by HITECH and associated federal rules and regulations.

“Agent” means those person(s) who are agents(s) of the Business Associate, in accordance with the Federal common law of agency, as referenced in 45 CFR § 160.402(c).

“Breach” means the acquisition, access, use or disclosure of protected health information (PHI) which compromises the security or privacy of the PHI, except as excluded in the definition of Breach in 45 CFR § 164.402.

“Business Associate shall have the meaning given in 45 CFR § 160.103.

“Individual” includes a person who qualifies as a personal representative in accordance with 45 CFR § 164.502(g).

“Protected Health Information” or PHI shall have the meaning given in 45 CFR § 160.103, limited to the information created or received by Business Associate from or on behalf of Agency.

“Security Incident” means any known successful or unsuccessful attempt by an authorized or unauthorized individual to inappropriately use, disclose, modify, access, or destroy any information or interference with system operations in an information system.

“Services” includes all work performed by the Business Associate for or on behalf of Covered Entity that requires the use and/or disclosure of protected health information to perform a business associate function described in 45 CFR § 160.103 under the definition of Business Associate.

“Subcontractor” means a person or organization to whom a Business Associate delegates a function, activity or service, other than in the capacity of a member of the workforce of the Business Associate. For purposes of this Agreement, the term Subcontractor includes Subgrantees.

**2. Identification and Disclosure of Privacy and Security Offices.** Business Associate and Subcontractors shall provide, within ten (10) days of the execution of this agreement, written notice to the Covered Entity’s contract/grant manager the names and contact information of both the HIPAA Privacy

Officer and HIPAA Security Officer. This information must be updated any time either of these contacts changes.

**3. Permitted and Required Uses/Disclosures of PHI.**

3.1 Except as limited in this Agreement, Business Associate may use or disclose PHI to perform Services, as specified in the underlying grant or contract with Covered Entity. The uses and disclosures of Business Associate are limited to the minimum necessary, to complete the tasks or to provide the services associated with the terms of the underlying agreement. Business Associate shall not use or disclose PHI in any manner that would constitute a violation of the Privacy Rule if used or disclosed by Covered Entity in that manner. Business Associate may not use or disclose PHI other than as permitted or required by this Agreement or as Required by Law.

3.2 Business Associate may make PHI available to its employees who need access to perform Services provided that Business Associate makes such employees aware of the use and disclosure restrictions in this Agreement and binds them to comply with such restrictions. Business Associate may only disclose PHI for the purposes authorized by this Agreement: (a) to its agents and Subcontractors in accordance with Sections 9 and 18 or, (b) as otherwise permitted by Section 3.

3.3 Business Associate shall be directly liable under HIPAA for impermissible uses and disclosures of the PHI it handles on behalf of Covered Entity, and for impermissible uses and disclosures, by Business Associate's Subcontractor(s), of the PHI that Business Associate handles on behalf of Covered Entity and that it passes on to Subcontractors.

**4. Business Activities.** Business Associate may use PHI received in its capacity as a Business Associate to Covered Entity if necessary for Business Associate's proper management and administration or to carry out its legal responsibilities. Business Associate may disclose PHI received in its capacity as Business Associate to Covered Entity for Business Associate's proper management and administration or to carry out its legal responsibilities if a disclosure is Required by Law or if Business Associate obtains reasonable written assurances via a written agreement from the person to whom the information is to be disclosed that the PHI shall remain confidential and be used or further disclosed only as Required by Law or for the purpose for which it was disclosed to the person, and the Agreement requires the person or entity to notify Business Associate, within two (2) business days (who in turn will notify Covered Entity within two (2) business days after receiving notice of a Breach as specified in Section 6.1), in writing of any Breach of Unsecured PHI of which it is aware. Uses and disclosures of PHI for the purposes identified in Section 3 must be of the minimum amount of PHI necessary to accomplish such purposes.

**5. Safeguards.** Business Associate, its Agent(s) and Subcontractor(s) shall implement and use appropriate safeguards to prevent the use or disclosure of PHI other than as provided for by this Agreement. With respect to any PHI that is maintained in or transmitted by electronic media, Business Associate or its Subcontractor(s) shall comply with 45 CFR sections 164.308 (administrative safeguards), 164.310 (physical safeguards), 164.312 (technical safeguards) and 164.316 (policies and procedures and documentation requirements). Business Associate or its Agent(s) and Subcontractor(s) shall identify in writing upon request from Covered Entity all of the safeguards that it uses to prevent impermissible uses or disclosures of PHI.

**6. Documenting and Reporting Breaches.**

6.1 Business Associate shall report to Covered Entity any Breach of Unsecured PHI, including Breaches reported to it by a Subcontractor, as soon as it (or any of its employees or agents)

becomes aware of any such Breach, and in no case later than two (2) business days after it (or any of its employees or agents) becomes aware of the Breach, except when a law enforcement official determines that a notification would impede a criminal investigation or cause damage to national security.

6.2 Business Associate shall provide Covered Entity with the names of the individuals whose Unsecured PHI has been, or is reasonably believed to have been, the subject of the Breach and any other available information that is required to be given to the affected individuals, as set forth in 45 CFR § 164.404(c), and, if requested by Covered Entity, information necessary for Covered Entity to investigate the impermissible use or disclosure. Business Associate shall continue to provide to Covered Entity information concerning the Breach as it becomes available to it. Business Associate shall require its Subcontractor(s) to agree to these same terms and conditions.

6.3 When Business Associate determines that an impermissible acquisition, use or disclosure of PHI by a member of its workforce is not a Breach, as that term is defined in 45 CFR § 164.402, and therefore does not necessitate notice to the impacted individual(s), it shall document its assessment of risk, conducted as set forth in 45 CFR § 402(2). When requested by Covered Entity, Business Associate shall make its risk assessments available to Covered Entity. It shall also provide Covered Entity with 1) the name of the person(s) making the assessment, 2) a brief summary of the facts, and 3) a brief statement of the reasons supporting the determination of low probability that the PHI had been compromised. When a breach is the responsibility of a member of its Subcontractor's workforce, Business Associate shall either 1) conduct its own risk assessment and draft a summary of the event and assessment or 2) require its Subcontractor to conduct the assessment and draft a summary of the event. In either case, Business Associate shall make these assessments and reports available to Covered Entity.

6.4 Business Associate shall require, by contract, a Subcontractor to report to Business Associate and Covered Entity any Breach of which the Subcontractor becomes aware, no later than two (2) business days after becomes aware of the Breach.

7. **Mitigation and Corrective Action.** Business Associate shall mitigate, to the extent practicable, any harmful effect that is known to it of an impermissible use or disclosure of PHI, even if the impermissible use or disclosure does not constitute a Breach. Business Associate shall draft and carry out a plan of corrective action to address any incident of impermissible use or disclosure of PHI. If requested by Covered Entity, Business Associate shall make its mitigation and corrective action plans available to Covered Entity. Business Associate shall require a Subcontractor to agree to these same terms and conditions.

8. **Providing Notice of Breaches.**

8.1 If Covered Entity determines that an impermissible acquisition, access, use or disclosure of PHI for which one of Business Associate's employees or agents was responsible constitutes a Breach as defined in 45 CFR § 164.402, and if requested by Covered Entity, Business Associate shall provide notice to the individual(s) whose PHI has been the subject of the Breach. When requested to provide notice, Business Associate shall consult with Covered Entity about the timeliness, content and method of notice, and shall receive Covered Entity's approval concerning these elements. The cost of notice and related remedies shall be borne by Business Associate.

8.2 If Covered Entity or Business Associate determines that an impermissible acquisition, access, use or disclosure of PHI by a Subcontractor of Business Associate constitutes a Breach as defined in 45 CFR § 164.402, and if requested by Covered Entity or Business Associate, Subcontractor shall provide notice to the individual(s) whose PHI has been the subject of the Breach. When Covered Entity requests that Business Associate or its Subcontractor provide notice, Business Associate shall either 1) consult with Covered Entity about the specifics of the notice as set forth in section 8.1, above, or 2) require, by contract, its Subcontractor to consult with Covered Entity about the specifics of the notice as set forth in section 8.1

8.3 The notice to affected individuals shall be provided as soon as reasonably possible and in no case later than 60 calendar days after Business Associate reported the Breach to Covered Entity.

8.4 The notice to affected individuals shall be written in plain language and shall include, to the extent possible, 1) a brief description of what happened, 2) a description of the types of Unsecured PHI that were involved in the Breach, 3) any steps individuals can take to protect themselves from potential harm resulting from the Breach, 4) a brief description of what the Business Associate is doing to investigate the Breach, to mitigate harm to individuals and to protect against further Breaches, and 5) contact procedures for individuals to ask questions or obtain additional information, as set forth in 45 CFR § 164.404(c).

8.5 Business Associate shall notify individuals of Breaches as specified in 45 CFR § 164.404(d) (methods of individual notice). In addition, when a Breach involves more than 500 residents of Vermont, Business Associate shall, if requested by Covered Entity, notify prominent media outlets serving Vermont, following the requirements set forth in 45 CFR § 164.406.

**9. Agreements with Subcontractors.** Business Associate shall enter into a Business Associate Agreement with any Subcontractor to whom it provides PHI received from Covered Entity or created or received by Business Associate on behalf of Covered Entity in which the Subcontractor agrees to the same restrictions and conditions that apply through this Agreement to Business Associate with respect to such PHI. Business Associate must enter into this Business Associate Agreement before any use by or disclosure of PHI to such agent. The written agreement must identify Covered Entity as a direct and intended third party beneficiary with the right to enforce any breach of the agreement concerning the use or disclosure of PHI. Business Associate shall provide a copy of the Business Associate Agreement it enters into with a subcontractor to Covered Entity upon request. Business associate may not make any disclosure of PHI to any Subcontractor without prior written consent of Covered Entity.

**10. Access to PHI.** Business Associate shall provide access to PHI in a Designated Record Set to Covered Entity or as directed by Covered Entity to an Individual to meet the requirements under 45 CFR § 164.524. Business Associate shall provide such access in the time and manner reasonably designated by Covered Entity. Within three (3) business days, Business Associate shall forward to Covered Entity for handling any request for access to PHI that Business Associate directly receives from an Individual.

**11. Amendment of PHI.** Business Associate shall make any amendments to PHI in a Designated Record Set that Covered Entity directs or agrees to pursuant to 45 CFR § 164.526, whether at the request of Covered Entity or an Individual. Business Associate shall make such amendments in the time and manner reasonably designated by Covered Entity. Within three (3) business days, Business Associate shall forward to Covered Entity for handling any request for amendment to PHI that Business Associate directly receives from an Individual.

**12. Accounting of Disclosures.** Business Associate shall document disclosures of PHI and all information related to such disclosures as would be required for Covered Entity to respond to a request by an Individual for an accounting of disclosures of PHI in accordance with 45 CFR § 164.528. Business Associate shall provide such information to Covered Entity or as directed by Covered Entity to an Individual, to permit Covered Entity to respond to an accounting request. Business Associate shall provide such information in the time and manner reasonably designated by Covered Entity. Within three (3) business days, Business Associate shall forward to Covered Entity for handling any accounting request that Business Associate directly receives from an Individual.

**13. Books and Records.** Subject to the attorney-client and other applicable legal privileges, Business Associate shall make its internal practices, books, and records (including policies and procedures and PHI) relating to the use and disclosure of PHI received from Covered Entity or created or received by Business Associate on behalf of Covered Entity available to the Secretary of HHS in the time and manner designated by the Secretary. Business Associate shall make the same information available to Covered Entity, upon Covered Entity's request, in the time and manner reasonably designated by Covered Entity so that Covered Entity may determine whether Business Associate is in compliance with this Agreement.

**14. Termination.**

14.1 This Agreement commences on the Effective Date and shall remain in effect until terminated by Covered Entity or until all of the PHI provided by Covered Entity to Business Associate or created or received by Business Associate on behalf of Covered Entity is destroyed or returned to Covered Entity subject to Section 19.8.

14.2 If Business Associate breaches any material term of this Agreement, Covered Entity may either: (a) provide an opportunity for Business Associate to cure the breach and Covered Entity may terminate the contract or grant without liability or penalty if Business Associate does not cure the breach within the time specified by Covered Entity; or (b) immediately terminate the contract or grant without liability or penalty if Covered Entity believes that cure is not reasonably possible; or (c) if neither termination nor cure are feasible, Covered Entity shall report the breach to the Secretary. Covered Entity has the right to seek to cure any breach by Business Associate and this right, regardless of whether Covered Entity cures such breach, does not lessen any right or remedy available to Covered Entity at law, in equity, or under the contract or grant, nor does it lessen Business Associate's responsibility for such breach or its duty to cure such breach.

**15. Return/Destruction of PHI.**

15.1 Business Associate in connection with the expiration or termination of the contract or grant shall return or destroy, at the discretion of the Covered Entity, all PHI received from Covered Entity or created or received by Business Associate on behalf of Covered Entity pursuant to this contract or grant that Business Associate still maintains in any form or medium (including electronic) within thirty (30) days after such expiration or termination. Business Associate shall not retain any copies of the PHI. Business Associate shall certify in writing for Covered Entity (1) when all PHI has been returned or destroyed and (2) that Business Associate does not continue to maintain any PHI. Business Associate is to provide this certification during this thirty (30) day period.

15.2 Business Associate shall provide to Covered Entity notification of any conditions that Business Associate believes make the return or destruction of PHI infeasible. If Covered Entity agrees that return or destruction is infeasible, Business Associate shall extend the protections of this Agreement to such PHI and limit further uses and disclosures of such PHI to those purposes that make the return or destruction infeasible for so long as Business Associate maintains such PHI. This shall also apply to all Agents and Subcontractors of Business Associate.

**16. Penalties.** Business Associate understands that: (a) there may be civil or criminal penalties for misuse or misappropriation of PHI and (b) violations of this Agreement may result in notification by Covered Entity to law enforcement officials and regulatory, accreditation, and licensure organizations.

**17. Training.** Business Associate understands that it is its obligation to comply with the law and shall provide appropriate training and education to ensure compliance with this Agreement. If requested by Covered Entity, Business Associate shall participate in AHS training regarding the use, confidentiality, and security of PHI, however, participation in such training shall not supplant nor relieve Business Associate of its obligations under this Agreement to independently assure compliance with the law and this Agreement.

**18. Security Rule Obligations.** The following provisions of this section apply to the extent that Business Associate creates, receives, maintains or transmits Electronic PHI on behalf of Covered Entity.

18.1 Business Associate shall implement and use administrative, physical, and technical safeguards in compliance with 45 CFR sections 164.308, 164.310, and 164.312 with respect to the Electronic PHI that it creates, receives, maintains or transmits on behalf of Covered Entity. Business Associate shall identify in writing upon request from Covered Entity all of the safeguards that it uses to protect such Electronic PHI.

18.2 Business Associate shall ensure that any Agent and Subcontractor to whom it provides Electronic PHI agrees in a written agreement to implement and use administrative, physical, and technical safeguards that reasonably and appropriately protect the Confidentiality, Integrity and Availability of the Electronic PHI. Business Associate must enter into this written agreement before any use or disclosure of Electronic PHI by such Agent or Subcontractor. The written agreement must identify Covered Entity as a direct and intended third party beneficiary with the right to enforce any breach of the agreement concerning the use or disclosure of Electronic PHI. Business Associate shall provide a copy of the written agreement to Covered Entity upon request. Business Associate may not make any disclosure of Electronic PHI to any Agent or Subcontractor without the prior written consent of Covered Entity.

18.3 Business Associate shall report in writing to Covered Entity any Security Incident pertaining to such Electronic PHI (whether involving Business Associate or an Agent or Subcontractor). Business Associate shall provide this written report as soon as it becomes aware of any such Security Incident, and in no case later than two (2) business days after it becomes aware of the incident. Business Associate shall provide Covered Entity with the information necessary for Covered Entity to investigate any such Security Incident.

18.4 Business Associate shall comply with any reasonable policies and procedures Covered Entity implements to obtain compliance under the Security Rule.

**19. Miscellaneous.**

19.1 In the event of any conflict or inconsistency between the terms of this Agreement and the terms of the contract/grant, the terms of this Agreement shall govern with respect to its subject matter. Otherwise, the terms of the contract/grant continue in effect.

19.2 Business Associate shall cooperate with Covered Entity to amend this Agreement from time to time as is necessary for Covered Entity to comply with the Privacy Rule, the Security Rule, or any other standards promulgated under HIPAA.

19.3 Any ambiguity in this Agreement shall be resolved to permit Covered Entity to comply with the Privacy Rule, Security Rule, or any other standards promulgated under HIPAA.

19.4 In addition to applicable Vermont law, the parties shall rely on applicable federal law (e.g., HIPAA, the Privacy Rule and Security Rule, and the HIPAA omnibus final rule) in construing the meaning and effect of this Agreement.

19.5 As between Business Associate and Covered Entity, Covered Entity owns all PHI provided by Covered Entity to Business Associate or created or received by Business Associate on behalf of Covered Entity.

19.6 Business Associate shall abide by the terms and conditions of this Agreement with respect to all PHI it receives from Covered Entity or creates or receives on behalf of Covered Entity even if some of that information relates to specific services for which Business Associate may not be a "Business Associate" of Covered Entity under the Privacy Rule.

19.7 Business Associate is prohibited from directly or indirectly receiving any remuneration in exchange for an individual's PHI. Business Associate will refrain from marketing activities that would violate HIPAA, including specifically Section 13406 of the HITECH Act. Reports or data containing the PHI may not be sold without Agency's or the affected individual's written consent.

19.8 The provisions of this Agreement that by their terms encompass continuing rights or responsibilities shall survive the expiration or termination of this Agreement. For example: (a) the provisions of this Agreement shall continue to apply if Covered Entity determines that it would be infeasible for Business Associate to return or destroy PHI as provided in Section 14.2 and (b) the obligation of Business Associate to provide an accounting of disclosures as set forth in Section 12 survives the expiration or termination of this Agreement with respect to accounting requests, if any, made after such expiration or termination.



**Appendix I – REQUIRED FORMS**  
**Department of Vermont Health Access**  
**Subcontractor Compliance Form**

Date: \_\_\_\_\_

Original Contractor/Grantee Name: \_\_\_\_\_

Contract/Grant #: \_\_\_\_\_

Subcontractor Name: \_\_\_\_\_

Amount Subcontracted: \_\_\_\_\_

Scope of Subcontracted Services: \_\_\_\_\_

\_\_\_\_\_  
\_\_\_\_\_  
\_\_\_\_\_  
\_\_\_\_\_  
\_\_\_\_\_

Is any portion of the work being outsourced outside of the United States?

☐ YES

☐ NO

(If yes, do not proceed)

All vendors under contract, grant, or agreement with the State of Vermont, are responsible for the performance and compliance of their subcontractors with the Standard State Terms and Conditions in Attachment C. This document certifies that the Vendor is aware of and in agreement with the State expectation and has confirmed the subcontractor is in full compliance (or has a compliance plan on file) in relation to the following:

- ☐ Subcontractor does not owe, is in good standing, or is in compliance with a plan for payment of any taxes due to the State of Vermont
- ☐ Subcontractor (if an individual) does not owe, is in good standing, or is in compliance with a plan for payment of Child Support due to the State of Vermont.
- ☐ Subcontractor is not on the State's disbarment list.

In accordance with State Standard Contract Provisions (Attachment C), the State may set off any sums which the subcontractor owes the State against any sums due the Vendor under this Agreement; provided, however, that any set off of amounts due the State of Vermont as taxes shall be in accordance with the procedures more specifically provided in Attachment C.

\_\_\_\_\_  
Signature of Subcontractor

\_\_\_\_\_  
Date

\_\_\_\_\_  
Signature of Vendor

\_\_\_\_\_  
Date

\_\_\_\_\_  
Received by DVHA Business Office

\_\_\_\_\_  
Date

**Required: Contractor cannot subcontract until this form has been returned to DVHA Contracts & Grants Unit.**