STATE OF VERMONT PARTICIPATING ADDENDUM # \_\_\_\_\_\_\_\_

PURCHASING PROGRAM: NASPO VALUEPOINT CLOUD SOLUTIONS

Led by the State of Utah

**Master Agreement** #\_\_\_\_\_\_\_\_

**Contractor:** \_\_\_\_\_\_\_\_

**Purchasing Program Webpage:** \_\_\_\_\_\_\_\_

**State Purchasing Entity**: Insert Requesting Agency or business unit

Purchasing Entity’s address for invoicing: \_\_\_\_\_\_\_\_\_\_\_

**Order No.** \_\_\_\_\_\_\_\_ (**This assigned Order # must be included on all correspondence, delivery documents and invoices**.)

1. **Scope.** This Order is a contract between the Contractor identified above (hereinafter the “Contractor”) and the State of Vermont, through its State Purchasing Entity identified above (hereinafter the “State”). Contractor hereby agrees to provide the Products and Services specified herein subject to and in accordance with the terms and conditions of the above-captioned Participating Addendum and Master Agreement (including respective amendments and attachments therewith), which are hereby incorporated by reference and shall apply to this Order as if specifically appended hereto. Capitalized terms used, but not defined herein, have the meanings ascribed to such terms in the Participating Addendum between the parties or otherwise in the Master Agreement between the Lead State and the Contractor.
2. **Time for Performance:** The term of this Order shall begin on \_\_\_\_\_\_\_\_\_ and end on \_\_\_\_\_\_\_\_\_\_ (the “Initial Term”).
3. **Payment Terms:** The maximum amount payable under this Order is $\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_. This maximum amount is not a guaranteed amount. Contractor shall submit invoices to the State Purchasing Entity’s address identified above. Payments shall be made only upon approval and acceptance by the State. Reimbursement of expenses is not authorized. All rates set forth in this Order shall be inclusive of any and all Contractor fees and expenses.
4. **Data Categorization and Type:** For purposes of this Order the parties have conferred and determined that the Contractor will hold, store, or process High Risk Data, Moderate Risk Data and/or Low Risk Data. In particular, the types of data that will be used by Contractor under this Order, include the following:

|  |  |
| --- | --- |
| **Type of Data** | **Applicable State & Federal** **Standards, Policies, and Laws**  |
| ☒ Publicly available information  | * [NIST 800-171](https://csrc.nist.gov/publications/detail/sp/800-171/rev-1/final)
 |
| ☐ Confidential Personally Identifiable Information (PII)  | * [State law on Notification of Security Breaches](http://legislature.vermont.gov/statutes/section/09/062/02435)
* [State Law on Social Security Number Protection](http://legislature.vermont.gov/statutes/section/09/062/02440)
* [State law on the Protection of Personal Information](https://legislature.vermont.gov/statutes/fullchapter/09/062)
* National Institute of Standards & Technology:  [NIST SP 800-53](https://nvd.nist.gov/800-53) Revision 4 “Moderate” risk controls
* [Privacy Act of 1974, 5 U.S.C. 552a](https://www.justice.gov/opcl/privacy-act-1974).
 |
| ☐ Payment Card Information   | * [Payment Card Industry Data Security Standard (PCI DSS)](https://www.pcisecuritystandards.org/document_library?category=pcidss&document=pci_dss) v 3.2
 |
| [x]  Federal Tax Information | * Internal Revenue Service Tax Information Security Guidelines for Federal, State and Local Agencies: [IRS Pub 1075](https://www.irs.gov/privacy-disclosure/safeguards-program)
 |

|  |  |
| --- | --- |
| **Type of Data** | **Applicable State & Federal** **Standards, Policies, and Laws**  |
| [ ]  Personal Health Information  (PHI) | * Health Insurance Portability and Accountability Act of 1996: [HIPAA](https://www.hhs.gov/hipaa/for-professionals/privacy/index.html)
* The Health Information Technology for Economic and Clinical Health Act [HITECH](https://www.hhs.gov/hipaa/for-professionals/special-topics/hitech-act-enforcement-interim-final-rule/index.html)
* [Code of Federal Regulations 45 CFR 95.621](https://www.govinfo.gov/app/collection/cfr/2017/title45)
 |
| [ ]  Affordable Care Act  Personally Identifiable  Information (PII) | * Internal Revenue Service Tax Information Security Guidelines for Federal, State and Local Agencies [IRS Pub 1075](https://www.irs.gov/privacy-disclosure/safeguards-program)
* Minimum Acceptable Risk Standards for Exchanges [MARS-E 2.0](https://www.cms.gov/CCIIO/Resources/Regulations-and-Guidance/)(Scroll down the page)
 |
| [ ]  Medicaid Information | * Medicaid Information Technology Architecture [MITA3.0](https://www.medicaid.gov/medicaid/data-and-systems/mita/mita-30/index.html)
* [Code of Federal Regulations 45 CFR 95.621](https://www.govinfo.gov/app/collection/cfr/2017/title45)
 |
| [ ]  Prescription Information | * [State law on the Confidentiality of Prescription Information](http://legislature.vermont.gov/statutes/section/18/091/04631)
 |
| [ ]  Student Education Data  | * Family Educational Rights and Privacy Act:  [FERPA](http://www2.ed.gov/policy/gen/guid/fpco/ferpa/index.html)
 |
| [ ]  Personal Information from  Motor Vehicle Records | * [Driver’s Privacy Protection Act](https://www.congress.gov/bill/103rd-congress/house-bill/3355/text) (Title XXX) (“DPPA”) 18 U.S.C. Chapter 123, §§ 2721 – 2725
 |
| [ ]  Criminal Records | * Criminal Justice Information Security Policy:  [CJIS](https://www.fbi.gov/about-us/cjis/cjis-security-policy-resource-center/view)
 |
| [ ]  Other:  *describe* | *[List what’s applicable or delete this line.]* |

1. **Products and Services Being Delivered:** The Contractor shall provide the Products and Services set forth in this Order in full satisfaction of the specific requirements of the Participating Addendum and this Order.

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| Awarded Category (PaaS, IaaS, or SaaS) | Product Name/SKU (Manufacturer) | Description | Vendor Part # | Quantity | Per Unit Cost | Total Price |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |

1. **Statement of Work:**
	1. Indicate each of the services pertaining to delivery or use of the software (e.g. configuration, customization, training, etc.) and include the following
		1. brief description of the work for each, with reference to any applicable exhibits
		2. Deliverable Date(s) or Phases
	2. For services performed at an hourly rate on a time and materials basis, State shall pay Contractor at the rate of $\_\_\_ per hour, however, total payment for services shall not exceed $\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_.
	3. The State shall retain 10% of each payment to hold until the satisfactory completion of [indicate applicable related service(s)] by the prescribed time and to the satisfaction of the State. Payment of retained fees shall occur [one month after the completion date upon receipt of invoicing from Contractor] [MODIFY AS NEEDED], provided State has accepted all applicable deliverables under this Purchase Order.
2. **Additional Terms and Conditions**: The Products and Services specified in this Order are as set forth subject to and shall comply with the following terms and conditions:
	1. Cloud service level terms and conditions applicable to the Products and Services specified in this Order are set forth in **Exhibit VT-Cloud** to this Order.
	2. Project Management services required for the Products and Services specified in this Order are set forth in **Exhibit VT-PM** to this Order.
	3. **Vermont Business Associate Agreement**: The terms and conditions of the State of Vermont Business Associate Agreement, as posted the Office of Purchasing & Contracting’s website at <https://bgs.vermont.gov/purchasing-contracting/forms> is hereby incorporated by reference and shall apply to this Order.
3. **Amendment:** This Order may not be amended except in a writing that is numbered and signed by the duly-authorized representatives of the State and the Contractor.
4. **Termination:** The State reserves the right to terminate this Order (a) for convenience upon written notice at least thirty (30) days in advance, (b) if appropriations are insufficient to support this Agreement after the project starts, or (c) due to unsatisfactory performance that is detailed in writing to the Contractor by the State and which remains uncured by the Contractor for more than fifteen (15) days following Contractor’s receipt of such written notice from the State, or such longer period of time specified in the notice, provided that the Contractor proceeds with reasonable diligence, as determined by the State, to completely cure. In the event the State cancels this Order for any of the preceding reasons, the State will pay for all completed and accepted deliverables up until the date of cancellation.
5. **No Implied Waivers:** No delay or failure to exercise any right, power or remedy accruing to either party upon breach or default by the other under this Order shall impair any such right, power or remedy, or shall be construed as a waiver of any such right, power or remedy nor shall any waiver of a single breach or default be deemed a waiver of any subsequent breach or default. All waivers must be in writing.
6. No terms, including a standard click-through license or website terms of use or privacy policy, shall apply to Purchasing unless Purchasing Entity has expressly agreed to such terms by appending them to a signed agreement. Further, and notwithstanding the foregoing sentence, in no event shall any terms: (a) require indemnification by the State of the Service Provider or a third party; (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.

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

**Certification Regarding Suspension or Debarment**. Contractor certifies under the pains and penalties of perjury that, as of the date this contract amendment is signed, neither Contractor nor Contractor’s principals (officers, directors, owners, or partners) are presently debarred, suspended, proposed for debarment, declared ineligible or excluded from participation in federal programs, or programs supported in whole or in part by federal funds. Contractor further certifies under pains and penalties of perjury that, as of the date this contract amendment is signed, Contractor is not presently debarred, suspended, nor named on the State’s debarment list at: <http://www.bgs.vermont.gov/purchasing-contracting/debarment>.

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

**REQUIRED PRIOR APPROVALS**

**This Order, regardless of value, shall be approved by the Vermont Chief Information Officer/Secretary of the Agency of Digital Services prior to execution.**

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

CIO Approval Date

**This Order, if valued at $25,000 or more per year, shall be certified by the Vermont Office of the Attorney General in accordance with 3 V.S.A. § 342 prior to execution.**

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

Certified by Date

**WE THE UNDERSIGNED PARTIES AGREE TO BE BOUND BY THIS AGREEMENT.**

<Insert Contractor Name>

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

Signature                                                                      Date

STATE OF VERMONT, <Insert Requesting Agency or business unit>

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

Signature                                                                      Date

# EXHIBIT VT-PM

#  PROJECT MANAGEMENT SERVICES

PROJECT MANAGEMENT APPROACH (change or remove as needed)

Describe the project management approach required by your agency or business unit.  If certain project management methodologies are to be employed and project progress reports and project team meetings are to take place, they need to also be defined as deliverables below.

PM APPROACH

The Contractor shall follow project management methodologies that are consistent with the Project Management Institute’s (PMI) *Project Management Body of Knowledge (PMBOK) Guide*.

Contractor staff will produce project deliverables using Microsoft Office products in v2007 or newer (Word, Excel, Project, Visio, etc.), and Adobe PDF, or other formats acceptable to the State.

**PROJECT DELIVERABLES**

Describe required deliverables in detail.  Under no circumstance should a SOW be developed or an SOW RFP be released where the deliverables are not quantified or the criteria for acceptance are not defined. Be clear and concise. The deliverables identified here should be directly tied to payment provisions.

Example: DELIVERABLE/ DELIVERY SCHEDULE

|  |  |  |
| --- | --- | --- |
| **ID** | **Deliverables** | **Expected Completion:** <If known> |
|  | Deliverable A |  |
|  | Deliverable B |  |
|  | Deliverable C |  |
|  |  |  |

Example: DELIVERABLES MATRIX

|  |  |  |  |
| --- | --- | --- | --- |
| **ID** | **Acceptance Criteria** | Est Completion Date | Quoted Cost |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  | Total |  |  |

**Exhibit VT-Cloud**

**I. Instructions for Exhibit VT-Cloud**

The terms and conditions appearing below in Section B of this Exhibit VT-Cloud are designed to be used for State procurements involving cloud services or “as-a-service” solutions. The terms of this Exhibit VT-Cloud are to be included in any RFP for a SaaS procurement and in any resulting contract or ordering document for SaaS.

*Review and edit Cloud Terms (Section B, below) before including with RFP or Contract/Order.* The procuring agency/department should review the Cloud Terms and revise as necessary to accomplish your specific business requirements.

The Cloud Terms are intended to accompany a vendor’s standard terms to prompt you to address customary State business requirements. The Cloud Terms must be tailored for the specific procurement. Understand that additional provision may be necessary and included with these Cloud Terms. Likewise, if the vendor’s standard terms sufficiently address a State business requirement, it is acceptable to remove the corresponding provision from the Cloud Terms and rely upon the vendor’s provision. In all cases, however, you should negotiate the vendor’s standard terms (typically found in a Subscription Agreement and Service Level Agreement) so that they meet State business requirements.

Below is a guide to reviewing and editing the Cloud terms prior to use; consult ADS or legal counsel for additional guidance.

*Guidelines for pre-posting review of Cloud Terms:*

A. Subscription Terms: Edits to this section are not required prior to use.

B. Support and Training: Edit this section to reflect actual support and training needs. For instance, is phone support needed 24x7 or only during business hours? Is online training required?

C. Service Levels: Edit this section to reflect actual service level requirements for the particular technology and technical needs.

Consider uptime needs (#1). Do you require 99.99% uptime, which allows approximately 5 minutes of unscheduled downtime per month? Is 99.9 sufficient (approximately 45 minutes per month)?

Edit #6 to define what “repeated or consistent failures” mean to you. Some examples: failure to achieve 99% uptime for two months in a six-month period; more than one severe defect in a month; failure to meet metrics for responding to defect reports for two consecutive months. It is critical to ensure that you have the right to terminate the agreement if service delivery becomes unacceptably bad. What constitutes an unacceptable level of performance that may cause you to terminate the contract?

D. Updates and Upgrades: Edit #2 and #3 if you require a different amount of notice for updates and upgrades. You may also delete #3 and #4 and substitute the following language: “Service Provider will notify Customer as far in advance as possible, and in any event at least thirty (30) days in advance, if any upcoming change to the Service will require Customer to modify its business environment or practices (e.g., currently supported browser is being phased out, workflow is being changed).”

E. Customer Data: Edits to this section are not required prior to use.

F. Data Privacy and Security:

YOU MUST CLASSIFY YOUR DATA by determining whether the vendor’s system will be transmitting, storing, or generating data that contains sensitive or personal information or information that is protected by law. Prior to contract execution, Service Provider and Customer must cooperate and hold a meeting to determine whether any sensitive or personal information will be stored or used in the Service that is subject to any law, rule or regulation providing for specific compliance obligations (e.g., HIPAA, FERPA, IRS Pub. 1075). If so, then Service Provider and Customer must review the Service specifications to determine whether the Service is appropriate for the level of sensitivity of the data to be stored or used in the Service, and Service Provider must document in the Agreement how the Service complies with such law

Edit #1 to explain what data will be in the system and why it is protected. Consult your agency’s legal counsel to determine which laws, if any, apply to the protection of this data. List these laws in #1 revising the “including but not limited to [list of laws]” at the end of the sentence. Examples: “social security numbers, driver’s license numbers, and financial account information in combination with a person’s name are protected personally identifiable information under Title 9 V.S.A. chapter 62”; student information is also protected under FERPA; health information is also protected under HIPAA. (This list is not intended to be complete. Note that multiple laws may apply.)

Edit #2 to reflect how the Service will comply with any such laws identified in #1. If Service Provider has separate documentation reflecting how the Service complies with applicable laws, this documentation should be attached to the contract and cross-referenced in #2.

G. Warranty: Consider whether you need a warranty for a time period (a 30-day warranty, for example) during which the vendor must repair defects. If so, you should add it here.

H. Subcontractors: Edits to this section are not required prior to use.

I. Disaster Recovery:

You may change the disaster recovery time period in #1.

Note that #2 of this section requires you to obtain documentation from the vendor showing how the vendor’s system supports your data protection requirements.

Determine whether your system is mission-critical. If it is, revise #3 to delete the words “If Customer designates the Service as mission-critical, as determined by Customer in its sole discretion.” If your system is not mission critical, delete #3.

J. Records and Audit: Edits to this section are not required prior to use.

L. Transition Assistance: Edits to this section are not required prior to use.

**DO NOT INCLUDE ABOVE INSTRUCTIONS IN ANY RFP OR CONTRACT/ORDERING DOCUMENT**

**II. State of Vermont Cloud Procurement Terms**

The following Exhibit VT-Cloud terms and conditions shall apply to all products and/or services provided by the Contractor (herein “Service Provider”) to the State (herein “Customer”).

**A. SUBSCRIPTION TERMS**

1. Service Provider grants to Customer a license or right to (i) access and use the Service, (ii) use underlying software as embodied or used in the service, and (iii) view, copy, download (if applicable), and use documentation.

2. No terms, including a standard click-through license or website terms of use or privacy policy, shall apply to Customer unless Customer has expressly agreed to such terms by appending them to a signed agreement. Further, in no event shall any terms: (a) require indemnification by the State of the Service Provider; (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.

**B. SUPPORT AND TRAINING**

1. Service Provider must provide technical support via online helpdesk and toll-free phone number, at minimum during Business Hours (Monday through Friday from 8:00 a.m. to 6:00 p.m. Eastern Time), and 24x7x365 if required by Customer and requested prior to contract execution.

2. Service Provider must make training available online to users.

3. All support and training shall be provided at no additional cost to Customer, except for customized support and training expressly requested by Customer.

**C. SERVICE LEVELS**

Service Provider must provide a Service Level Agreement (SLA) that contains, at minimum, the following terms:

Uptime; scheduled maintenance

1. SLA must include (1) a specified guaranteed annual or monthly uptime percentage, at minimum 99.99%; and (2) a definition of uptime and how it is calculated.

2. For purposes of calculating uptime percentage, scheduled maintenance may be excluded up to ten (10) hours per month, but unscheduled maintenance and any scheduled maintenance in excess of ten (10) hours must be included as downtime

3. Scheduled maintenance must occur: with at least two (2) business days’ advance notice; at agreed-upon times when a minimum number of users will be using the system; and in no event during Business Hours.

Defects; other SLA metrics

4. SLA must include: (1) response and resolution times for defects; (2) at least three levels of defect classifications (severe, medium, low); and (3) any other applicable performance metrics (e.g., latency, transaction time or system speeds) based on industry standards.

5. While the Service Provider may initially classify defects, Customer determines final classification of defects.

Remedies

6. SLA must include remedies for failure to meet guaranteed uptime percentage, response and resolution times, and other metrics, which may include fee reductions and extensions in service period at no cost.

7. Repeated or consistent failures to meet SLA metrics result in (1) a refund of all fees paid by Customer for the period in which the failure occurred; (2) participation by Service Provider in a root cause analysis and corrective action plan at Customer’s request; and (3) a right for Customer to terminate without penalty and without waiver of any rights upon written notice to Service Provider.

Reports

8. Service Provider will provide Customer with a written report (which may be electronic) of performance metrics, including uptime percentage and record of service support requests, classifications, and response and resolution times, at least quarterly or as requested by Customer. Service Provider shall maintain accurate, reasonably detailed records pertaining to Service Levels, including service availability and downtime. Customer may independently audit the report at Customer’s expense.

9. Representatives of Service Provider and Customer shall meet as often as may be reasonably requested by either party to review the performance of the Service and to discuss technical plans, financial matters, system performance, service levels, and any other matters related to this Agreement.

10. Service Provider will provide to Customer regular status reports during unscheduled downtime, at least twice per day or upon request

11. Service Provider will provide Customer with root cause analysis within thirty (30) days of unscheduled downtime at no additional cost

**D. UPDATES AND UPGRADES**

1. Service Provider will make updates and upgrades available to Customer at no additional cost when Service Provider makes such updates and upgrades generally available to its users.

2. Service Provider will notify Customer at least sixty (60) days in advance prior to any major update or upgrade.

3. Service Provider will notify Customer at least five (5) business days in advance prior to any minor update or upgrade, including hotfixes and installation of service packs, except in the case of an emergency such as a security breach.

4. No update, upgrade or other change to the Service may decrease the Service’s functionality, adversely affect Customer’s use of or access to the Service, or increase the cost of the Service to Customer.

**E. CUSTOMER DATA**

1. Customer retains full right and title to data provided by Customer and any data derived therefrom, including metadata (collectively, the “Customer Data”).

2. Service Provider shall not collect, access, or use user-specific Customer Data except as strictly necessary to provide Service to Customer. No information regarding Customer’s use of the Service may be disclosed, provided, rented or sold to any third party for any reason unless required by law or regulation or by an order of a court of competent jurisdiction. This obligation shall extend beyond the term of the Agreement in perpetuity.

3. Service Provider shall not use any information collected in connection with the Agreement, including the Customer Data, for any purpose other than fulfilling its obligations under the Agreement.

4. At no time may any Data or processes which either belong to Customer, or are intended for Customer’s exclusive use, be copied, disclosed, or retained by Service Provider for subsequent use in any transaction that does not include Customer.

5. Customer Data must remain at all times within the continental United States. Service Provider must disclose to Customer the identity of any third-party host of Customer Data prior to the signing of this Agreement.

6. Customer shall have access to the Customer Data at any time during the term of the Agreement or for up to three (3) months after the term (so long as the Customer Data remains in the Service Provider’s possession). Within ten (10) business days of a request by Customer, the Service Provider will make available to Customer a complete and secure (i.e. encrypted and appropriately authenticated) download file of Customer Data in a format acceptable to Customer including all schema and transformation definitions and/or delimited text files with documented, detailed schema definitions along with attachments in their native format. *Provided, however*, in the event the Service Provider 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 Service Provider shall immediately return all Customer Data to Customer control; including, but not limited to, making all necessary access to applicable remote systems available to the Customer for purposes of downloading all Customer Data. The Service Provider’s policies regarding the retrieval of data upon the termination of services have been made available to the Customer upon execution of this Agreement under separate cover. The Service Provider shall provide the Customer with not less than thirty (30) days advance written notice of any material amendment or modification of such policies.

7. Upon termination of this Agreement for any reason whatsoever, Service Provider shall immediately deliver to Customer all Customer Data (including without limitation any Deliverables for which Customer has made payment in whole or in part), that are in the possession or under the control of Service Provider in whatever stage of development and form of recordation such Customer property is expressed or embodied at that time.

8. Three (3) months after the termination or expiration of the Agreement or upon Customer’s earlier written request, and in any event after Customer has had an opportunity to export and recover the Customer Data, Service Provider shall at its own expense destroy and erase from all systems it directly or indirectly uses or controls, in a manner that assures the State that the information is rendered unrecoverable, all tangible or intangible forms of the Customer Data and Customer’s Confidential Information, in whole or in part, and all copies thereof except such records as are required by law. To the extent that any applicable law prevents Service Provider from destroying or erasing Customer Data as described in the preceding sentence, Service Provider shall retain, in its then current state, all such Customer Data then within its right of control or possession in accordance with the confidentiality, security and other requirements of this Agreement, and perform its obligations under this section as soon as such law no longer prevents it from doing so. Service Provider shall, upon request, send a written certification to Customer certifying that it has destroyed the Customer Data and Confidential Information in compliance with this section.

**F. DATA PRIVACY AND SECURITY**

1. Service Provider must comply with all applicable laws related to data privacy and security, as may be amended from time to time, including, but not limited to, Chapter 62 of Title 9 of the Vermont Statutes, HIPAA, HITECH, FERPA and/or IRS Pub. 1075.

2. If “personally identifiable information,” as defined in 9 V.S.A. §2430(5), will be stored or used in the Service, then Service Provider is a “data collector” as such term is defined in Chapter 62 of Title 9 of the Vermont Statutes (9 V.S.A. §2430(3)).

3. Service Provider shall provide a secure environment for Customer Data, and any hardware and software, including servers, network and data components provided by Service Provider as part of its performance under this Agreement, in order to protect, and prevent unauthorized access to and use or modification of, the Service and Customer Data. The Service Provider represents and warrants that it has implemented and it shall maintain during the term of this Contract the highest industry standard administrative, technical, and physical safeguards and controls consistent with NIST *Special Publication 800-53* (version 4 or higher) and *Federal Information Processing Standards Publication* 200 and designed to (i) ensure the security and confidentiality of Customer Data; (ii) protect against any anticipated security threats or hazards to the security or integrity of the Customer Data; and (iii) protect against unauthorized access to or use of Customer Data. Such measures shall include at a minimum: (1) access controls on information systems, including controls to authenticate and permit access to Customer Data only to authorized individuals and controls to prevent the Service Provider employees from providing Customer Data to unauthorized individuals who may seek to obtain this information (whether through fraudulent means or otherwise); (2) industry-standard firewall protection; (3) encryption of electronic Customer Data while in transit from the Service Provider networks to external networks; (4) measures to store in a secure fashion all Customer 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 Customer Data; (6) measures to ensure that the Customer 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 Customer 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 Service Provider systems that are used in the provision of the services against intrusion on a twenty-four (24) hour a day basis.

4. Customer Data must be partitioned from other data in such a manner that access to it will not be impacted or forfeited due to e-discovery, search and seizure or other actions by third parties obtaining or attempting to obtain Service Provider’s records, information or data for reasons or activities that are not directly related to Customer’s business.

5. Service Provider shall not access Customer user accounts, or Customer Data, except in the course of data center operations, response to service or technical issues, as required by the express terms of this Agreement, or at Customer’s written request.

6. Service Provider may not share Customer Data with its parent company or other affiliate without Customer’s express written consent.

7. In the event of any breach of the Service’s security that adversely affects Customer Data or Service Provider’s obligations with respect thereto, or any evidence that leads Service Provider to reasonably believe that such a breach is imminent, Service Provider shall immediately (and in no event more than twenty-four hours after discovering such breach) notify Customer. Service Provider shall identify the affected Customer Data and inform Customer of the actions it is taking or will take to reduce the risk of further loss to Customer. Service Provider shall provide Customer the opportunity to participate in the investigation of the breach and to exercise control over reporting the unauthorized disclosure. The Service Provider shall provide such other information, including a written report, as reasonably requested by the Customer.

8. In the event that personally identifiable information is compromised, Service Provider shall be responsible for providing breach notification to the affected individuals in coordination with the State.

9. Service Provider shall fully indemnify, defend, and save harmless the Customer from and against any and all fines, criminal or civil penalties, judgments, damages and assessments, including reasonable expenses suffered by, accrued against, charged to or recoverable from the State resulting from a security breach or the unauthorized disclosure of Customer Data by the Service Provider, its officers, agents, employees, and subcontractors.

**G. WARRANTY**

In addition to the warranties set forth in the Participating Addendum, Service Provider warrants that:

1. Service Provider will provide to Customer commercially reasonable continuous and uninterrupted access to the Service, and will not interfere with Customer’s access to and use of the Service during the term of this Agreement.

2. The Service is compatible with and will operate successfully with any environment (including web browser and operating system) specified by Service Provider in its documentation.

**H. SUBCONTRACTORS**

1. Before and during the term of this Agreement, Service Provider must notify Customer prior to any subcontractor providing any services, directly or indirectly, to Customer under this Agreement that materially affect the Service being provided to Customer, including: hosting; data storage; security and data integrity; payment; and disaster recovery. Customer must approve all such subcontractors identified after the effective date of the Agreement.

2. Service Provider is responsible for its subcontractors’ compliance with the Agreement, and shall be fully liable for the actions and omissions of subcontractors as if such actions or omissions were performed by Service Provider.

**I. DISASTER RECOVERY**

1. Service Provider agrees to maintain and follow a disaster recovery plan designed to maintain Customer access to the Service, and to prevent the unintended destruction or loss of Customer Data. The disaster recovery plan shall provide for and be followed by Service Provider such that in no event shall the Service be unavailable to Customer for a period in excess of twenty-four (24) hours.

2. The Service Provider’s back-up policies have been made available to the Customer upon execution of this Agreement under separate cover. The Service Provider shall provide the State with not less than thirty (30) days advance written notice of any material amendment or modification of such policies.

3. If Customer designates the Service as mission-critical, as determined by Customer in its sole discretion: (1) Service Provider shall review and test the disaster recovery plan regularly, at minimum twice annually; (2) Service Provider shall back up Customer Data no less than twice daily in an off-site “hardened” facility located within the continental United States; and (3) in the event of Service failure, Service Provider shall be able to restore the Service, including Customer Data, with loss of no more than twelve (12) hours of Customer Data and transactions prior to failure.

**J. RECORDS AND AUDIT**. In addition to requirements set forth in the Participating Addendum:

1. Examination and Audit. Service Provider will maintain and cause its permitted contractors to maintain a complete audit trail of all transactions and activities, financial and non-financial, in connection with this Contract. Service Provider will provide to the Customer, its internal or external auditors, clients, inspectors, regulators and other designated representatives, at reasonable times (and in the case of State or federal regulators, at any time required by such regulators) access to Service Provider personnel and to any and all Service Provider facilities or where the required information, data and records are maintained, for the purpose of performing audits and inspections (including unannounced and random audits) of Service Provider and/or Service Provider personnel and/or any or all of the records, data and information applicable to this Contract. At a minimum, such audits, inspections and access shall be conducted to the extent permitted or required by any laws applicable to the Customer or Service Provider (or such higher or more rigorous standards, if any, as Customer or Service Provider applies to its own similar businesses, operations or activities), to (i) verify the accuracy of charges and invoices; (ii) verify the integrity of Customer Data and examine the systems that process, store, maintain, support and transmit that data; (iii) examine and verify Service Provider’s and/or its permitted contractors’ operations and security procedures and controls; (iv) examine and verify Service Provider’s and/or its permitted contractors’ disaster recovery planning and testing, business resumption and continuity planning and testing, contingency arrangements and insurance coverage; and (v) examine Service Provider’s and/or its permitted contractors’ performance of the Services including audits of: (1) practices and procedures; (2) systems, communications and information technology; (3) general controls and physical and data/information security practices and procedures; (4) quality initiatives and quality assurance, (5) contingency and continuity planning, disaster recovery and back-up procedures for processes, resources and data; (6) Service Provider’s and/or its permitted contractors’ efficiency and costs in performing Services; (7) compliance with the terms of this Contract and applicable laws, and (9) any other matters reasonably requested by the Customer. Service Provider 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, including the installation and operation of audit software.

2. Software Licensee Compliance Report. Upon request and not more frequently than annually, the State will provide Service Provider with a certified report concerning the State’s use of any software licensed for State use pursuant this Contract. The parties agree that any non-compliance indicated by the report shall not constitute infringement of the licensor’s intellectual property rights, and that settlement payment mutually agreeable to the parties shall be the exclusive remedy for any such non-compliance.

3. Operations Security. The Service Provider shall cause an SSAE 18 SOC 2 Type 2 audit report to be conducted annually. The audit results and the Service Provider’s plan for addressing or resolution of the audit results shall be shared with the Customer within sixty (60) days of the Service Provider 's receipt of the audit results. Further, on an annual basis, within 90 days of the end of the Service Provider’s fiscal year, the Service Provider shall transmit its annual audited financial statements to the State.

**K. TRANSITION ASSISTANCE**

1. Service Provider shall reasonably cooperate with other parties in connection with all services to be delivered under this Agreement, including without limitation any successor provider to whom Customer Data is to be transferred in connection with termination. Service Provide shall assist Customer in exporting and extracting the Customer Data, in a format usable without the use of the Service and as agreed to by Customer, at no additional cost. Any transition services requested by Customer involving additional knowledge transfer and support may be subject to a separate transition SOW on a time and materials basis either for a fixed fee or at rates to be mutually agreed upon by the parties.

2. If Customer determines in its sole discretion that a documented transition plan is necessary, then no later than sixty (60) days prior to termination, Service Provider and Customer shall jointly create a written Transition Plan Document identifying transition services to be provided and including a SOW if applicable. Both parties shall comply with the Transition Plan Document both prior to and after termination as needed.