NASPO VALUEPOINT CLOUD SOLUTIONS 2016-2026

MASTER SERVICES AGREEMENT NO. AR2472

OREGON PARTICIPATING ADDENDUM #9412

AMENDMENT NO. 1

This is Amendment No. 1 to Oregon Participating Addendum #9412 effective April 1, 2019, as amended from time to time ("Participating Addendum") between the State of Oregon, acting by and through its Department of Administrative Services ("DAS PS"), on behalf of state agencies and members of the Oregon Cooperative Purchasing Program ("Authorized Purchaser") and Carahsoft Technology Corp. ("Contractor"). This Amendment is effective upon signature by the parties ("Amendment Effective Date").

The parties agree to amend the Participating Addendum, as follows:

1. For the purposes of this Participating Addendum, "Master Agreement" means the agreement entered into between the State of Utah ("Lead State") on behalf of the member states of the NASPO Value Point Procurement Cooperative ("NASPO ValuePoint") and Contractor effective October 14, 2016, No. AR2472, including the State of Utah Cooperative Contract and Attachments A through E and all amendments to the agreement, as may be entered into between the Lead State and Contractor from time to time.

2. For the purposes of Amendment No. 6 to the Master Agreement, effective November 7, 2017 and for the avoidance of doubt, the IBM Cloud Services Agreement incorporated into the Master Agreement as an Attachment E to the Master Agreement specifically includes the following documents, attached hereto as Attachment A:

- Cloud Services Agreement, Z126-6304-US-7 05-2017.docx
- Terms of Use, General Terms for Cloud Offerings, i126-5948-08 (06/2019)
- Data Security and Privacy Principles for IBM Cloud Services, Z126-7745-WW-3-05-2018
- Data Processing Addendum, Z126-7870-02 03-2019 DPA

Except as expressly amended above, all other terms and conditions of the Participating Addendum are still in full force and effect. Contractor certifies that the representations, warranties and certifications contained in the Participating Addendum are true and correct as of the Amendment Effective Date and with the same effect as though made at the time of execution of the Participating Addendum.

Certification: The individual signing on behalf of Contractor hereby certifies under penalty of perjury: (a) the number shown on this form is Contractor's correct taxpayer identification; (b) Contractor is not subject to backup withholding because (i) Contractor is exempt from backup withholding, (ii) Contractor has not been notified by the IRS that Contractor is subject to backup withholding as a result of a failure to report all interest or dividends, or (iii) the IRS has notified Contractor that Contractor is no longer subject to backup withholding; (c) s/he is authorized to act on behalf of Contractor, s/he has authority and knowledge regarding Contractor's payment of taxes, and to the best of her/his knowledge, for a period of no fewer than six calendar years preceding the Amendment Effective Date, Contractor has faithfully has complied with and is not in violation of: (i) all tax laws of this state, including but not limited to ORS 305.620 and ORS chapters 316, 317, and 318;(ii) any tax provisions imposed by a political subdivision of this state that applied to Contractor, to Contractor's property, operations, receipts, or income, or to Contractor's performance of or compensation for any work performed by Contractor; (iii) any tax provisions imposed by a political subdivision of this state that applied to Contractor, or to goods, services, or property, whether tangible or intangible, provided by Contractor; and (iv) any rules, regulations, charter provisions, or ordinances that implemented or enforced any of the foregoing tax laws or provisions; and;. (d) Contractor is an independent contractor as defined in ORS 670.600; and (e) the supplied Contractor data is true and accurate.

Carahsoft Technology Corp:

By: Kristina Smith

Title: Director of Contracts

Date: 10/31/2019

FEID: 52-2189693

THE STATE OF OREGON, acting
by and through the Department of
Administrative Services

By: Lori Nordli

Title: IT Procurement Strategist

Date: 10/31/19

NASPO VALUEPOINT CLOUD SOLUTIONS 2016-2026
MASTER SERVICES AGREEMENT NO. AR2472
OREGON PARTICIPATING ADDENDUM #9412
AMENDMENT NO. 1 - Attachment A

Cloud Services Agreement

This Cloud Services Agreement (CSA) and applicable Attachments and Transaction Documents (TDs) are the complete agreement regarding transactions under this CSA (together, the "Agreement") under which Client may order Cloud Services. Attachments typically contain additional terms that apply to similar types of offerings. TDs, such as service descriptions, order documents or statements of work, contain specific details related to an order for a Cloud Service and there may be more than one TD providing the details of an order. In the event of conflict, an Attachment prevails over this CSA and a TD prevails over both the CSA and any Attachment.

1. Cloud Services

a. A Cloud Service is an IBM branded offering provided by IBM and made available via a network. Each Cloud Service is described in an Attachment or a TD. Cloud Services are designed to be available 24/7, subject to maintenance. Client will be notified of scheduled maintenance. Technical support and service level commitments, if applicable, are specified in an Attachment or TD.

b. Client accepts an Attachment or TD by ordering, enrolling, using, or making a payment for the Cloud Service. When IBM accepts Client's order, IBM provides Client the authorizations specified in the TD. The term, including any renewal term, for a Cloud Service is described in an Attachment or TD.

c. IBM will provide the facilities, personnel, equipment, software, and other resources necessary to provide the Cloud Services and generally available user guides and documentation to support Client's use of the Cloud Service. Client will provide hardware, software and connectivity to access and use the Cloud Service, including any required Client-specific URL addresses and associated certificates. An Attachment or TD may have additional Client responsibilities.

d. Client may access a Cloud Service only to the extent of authorizations acquired by Client. Client is responsible for use of Cloud Services by any user who accesses the Cloud Service with Client's account credentials. A Cloud Service may not be used in any jurisdiction for unlawful, obscene, offensive or fraudulent Content or activity, such as advocating or causing harm, interfering with or violating the integrity or security of a network or system, evading filters, sending unsolicited, abusive, or deceptive messages, viruses or harmful code, or violating third party rights. If there is a complaint or notice of violation, use may be suspended until resolved, and terminated if not resolved promptly. Client may not i) resell direct access to a Cloud Service to a third party outside Client's Enterprise; or ii) combine Cloud Services with Client's value add to create a commercially available Client branded solution for which Client charges a fee.

2. Content and Data Protection

a. Content consists of all data, software, and information that Client or its authorized users provides, authorizes access to, or inputs to the Cloud Service. Use of the Cloud Service will not affect Client's existing ownership or license rights in such Content. IBM and its contractors, and subprocessors may access and use the Content solely for the purpose of providing and managing the Cloud Service, unless otherwise described in a TD.

b. Client is responsible for obtaining all necessary rights and permissions to enable, and grants such rights and permissions to, IBM, and its contractors and subprocessors to use, provide, store and process Content in the Cloud Service. This includes Client making necessary disclosures and obtaining consent, if required, before providing individuals' information, including personal or other regulated information in such Content. If any Content could be subject to governmental regulation or may require security measures beyond those specified by IBM for an offering, Client will not input, provide, or allow such Content unless specifically permitted in the terms of the relevant TD or unless IBM has otherwise first agreed in writing to implement additional security and other measures.

c. Upon request by either party, IBM, Client or their affiliates will enter into additional agreements as required by law in the prescribed form for the protection of personal or regulated personal data included in Content. The parties agree (and will ensure that their respective affiliates agree) that such additional agreements will be subject to the terms of the Agreement.

d. IBM will return or remove Content from IBM computing resources upon the expiration or cancellation of the Cloud Service, or earlier upon Client's request. IBM may charge for certain activities performed at Client's request (such as delivering Content in a specific format). IBM does not archive Content, however some Content may remain in Cloud Service backup files until expiration of such files as governed by IBM's backup retention practices.

e. Each Cloud Service is designed to protect Content as described in the Agreement. IBM's Data Security and Privacy Principles for IBM Cloud Services (DSP), at http://www.ibm.com/cloud/data-security, apply for generally available Cloud Service offerings or as described in the applicable TD. IBM will treat all Content as confidential by not disclosing Content except to IBM employees, contractors, and subprocessors, and only to the extent necessary to deliver the Cloud Service, unless otherwise specified in a TD. Specific security features and functions of a Cloud Service may be provided in an Attachment and TDs. Client is responsible to assess the suitability of each Cloud Service for Client's intended use and Content. By using the Cloud Service, Client acknowledges that it meets Client's requirements and processing instructions.

f. Client acknowledges that i) IBM may modify the DSP from time to time at IBM's sole discretion and ii) such modifications will supersede prior versions. The intent of any modification to the DSP will be to i) improve or clarify existing commitments, ii) maintain alignment to current adopted standards and applicable laws, or iii) provide additional commitments. No modification to the DSP will materially degrade the security of a Cloud Service.

3. Changes

a. IBM may modify a Cloud Service, without degrading its functionality or security features.

b. IBM may withdraw a Cloud Service on 12 months' notice, unless otherwise stated in a TD. IBM will continue to provide the Cloud Service for the remainder of Client's unexpired term or work with Client to migrate to another IBM offering.

c. Since this CSA may apply to many future orders, IBM may modify this CSA by providing Client at least three months' written notice. Changes are not retroactive; they apply, as of the effective date, only to new orders, ongoing Cloud Services that do not expire, and renewals. For transactions with a defined renewable contract period, Client may request that IBM defer the change effective date until the end of the current contract period. Client accepts changes by placing new orders or continuing use after the change effective date or allowing transactions to renew after receipt of the change notice. Except as provided above, all changes to the Agreement must be in writing accepted by both parties.

4. Warranties

a. IBM warrants that it provides Cloud Services using commercially reasonable care and skill in accordance with the applicable Attachment or TD. The warranty for a Cloud Service ends when the Cloud Service ends.

b. **IBM does not warrant uninterrupted or error-free operation of a Cloud Service or that IBM will correct all defects or prevent third party disruptions or unauthorized third party access. These warranties are the exclusive warranties from IBM and replace all other warranties, including the implied warranties or conditions of satisfactory quality, merchantability, non-infringement, and fitness for a particular purpose. IBM warranties will not apply if there has been misuse, modification, damage not caused by IBM, failure to comply with instructions provided by IBM, or if otherwise stated in an Attachment or TD. Non-IBM services are sold under the Agreement as-is, without warranties of any kind.** Third parties may provide their own warranties to Client.

5. Charges, Taxes, and Payment

a. Client agrees to pay all applicable charges specified for a Cloud Service, charges for use in excess of authorizations, and any late payment fees. Charges are exclusive of any customs or other duty, tax, and similar levies imposed by any authority resulting from Client's acquisitions under the Agreement and will be invoiced in addition to such charges. Amounts are due upon receipt of the invoice and payable within 30 days of the invoice date to an account specified by IBM. Prepaid Services must be used within the applicable period. IBM does not give credits or refunds for any prepaid, one-time charges, or other charges already due or paid. IBM may change charges on thirty days' notice or as specified in a TD. Where taxes are based upon the location(s) receiving the benefit of the Cloud Service, Client has an ongoing obligation to notify IBM of such location(s) if different than Client's business address listed in the applicable Attachment or TD.

b. Client agrees to: i) pay withholding tax directly to the appropriate government entity where required by law; ii) furnish a tax certificate evidencing such payment to IBM; iii) pay IBM only the net proceeds after tax; and iv) fully cooperate with IBM in seeking a waiver or reduction of such taxes and promptly complete and file all relevant documents.

6. Liability and Indemnity

a. IBM's entire liability for all claims related to the Agreement will not exceed the amount of any actual direct damages incurred by Client up to the amounts paid (if recurring charges, up to 12 months' charges apply) for the service that is the subject of the claim, regardless of the basis of the claim. IBM will not be liable for special, incidental, exemplary, indirect, or economic consequential damages, or lost profits, business, value, revenue, goodwill, or anticipated savings. These limitations apply collectively to IBM, its affiliates, contractors, subprocessors, and suppliers.

b. The following amounts are not subject to the above cap: i) third party payments referred to in the paragraph below; and ii) damages that cannot be limited under applicable law.

c. If a third party asserts a claim against Client that an IBM Service acquired under the Agreement infringes a patent or copyright, IBM will defend Client against that claim and pay amounts finally awarded by a court against Client or included in a settlement approved by IBM, provided that Client promptly (i) notifies IBM in writing of the claim, (ii) supplies information requested by IBM, and (iii) allows IBM to control, and reasonably cooperates in, the defense and settlement, including mitigation efforts.

d. IBM has no responsibility for claims based on non-IBM products and services, items not provided by IBM, or any violation of law or third party rights caused by Client's Content, materials, designs, or specifications.

7. Termination

a. IBM may suspend, revoke or limit Client's use of a Cloud Service if IBM determines there is a material breach of Client's obligations, a security breach, or violation of law. If the cause of the suspension can reasonably be remedied, IBM will provide notice of the actions Client must take to reinstate the Cloud Service. If Client fails to take such actions within a reasonable time, IBM may terminate the Cloud Service. Failure to pay is a material breach.

b. Either party may terminate this CSA: i) without cause on at least one month's notice to the other after expiration or termination of its obligations under the Agreement; or ii) immediately for cause if the other is in material breach of the Agreement, provided the one who is not complying is given notice and reasonable time to comply. Any terms that by their nature extend beyond the Agreement termination remain in effect until fulfilled, and apply to successors and assignees. Termination of this CSA does not terminate TDs, and provisions of this CSA as they relate to such TDs remain in effect until fulfilled or otherwise terminated in accordance with their terms.

c. Client may terminate a Cloud Service on one month's notice: (i) at the written recommendation of a government or regulatory agency following a change in either applicable law or the Cloud Services; (ii) if IBM's modification to the computing environment used to provide the Cloud Service causes Client to be noncompliant with applicable laws; or (iii) if IBM notifies Client of a modification that has a material adverse effect on Client's use of the Cloud Service, provided that IBM will have 90 days to work with Client to minimize such effect. In the event of such termination, IBM shall refund a portion of any prepaid amounts for the applicable Cloud Service for the period after the date of termination. If the Agreement is terminated for any other reason, Client shall pay to IBM, on the date of termination, the total amounts due per the Agreement. Upon termination, IBM may assist Client in transitioning Client's Content to an alternative technology for an additional charge and under separately agreed terms.

8. Governing Laws and Geographic Scope

a. Each party is responsible for complying with: i) laws and regulations applicable to its business and Content; and ii) import, export and economic sanction laws and regulations, including defense trade control regime of any jurisdiction, including the International Traffic in Arms Regulations and those of the United States that prohibit or restrict the export, re-export, or transfer of products, technology, services or data, directly or indirectly, to or for certain countries, end uses or end users. Client is responsible for its use of IBM and non-IBM products and services.

b. Both parties agree to the application of the laws of the State of New York, United States, without regard to conflict of law principles. The rights and obligations of each party are valid only in the country of Client's business address. If Client or any user exports or imports Content or use of any portion of the Cloud Service outside the country of Client's business address, IBM will not serve as the exporter or importer. If any provision of the Agreement is invalid or unenforceable, the remaining provisions remain in full force and effect. Nothing in the Agreement affects statutory rights of consumers that cannot be waived or limited by contract. The United Nations Convention on Contracts for the International Sale of Goods does not apply to transactions under the Agreement.

9. General

a. IBM is an independent contractor, not Client's agent, joint venturer, partner, or fiduciary, and does not undertake to perform any of Client's regulatory obligations, or assume any responsibility for Client's business or operations. Each party is responsible for determining the assignment of its personnel, and all contractors and subprocessors, and for their direction, control, and compensation.

b. IBM maintains a robust set of business conduct and related guidelines covering conflicts of interest, market abuse, anti-bribery & corruption, and fraud. IBM and its personnel comply with such policies and require contractors and subprocessors to have similar policies.

c. Account Data is information Client provides to IBM, other than Content, about Client or its users that IBM needs to enable Client's use of a Cloud Service or information concerning such use. IBM, its contractors and subprocessors may process, store and use Account Data wherever they do business to enable product features, administer use, personalize experience, and otherwise support or improve use of the Cloud Service as described in IBM's Online Privacy Statement.

d. IBM Business Partners who use or make available IBM Cloud Services are independent from IBM and unilaterally determine their prices and terms. IBM is not responsible for their actions, omissions, statements, or offerings.

e. Neither party may assign the Agreement, in whole or in part, without the prior written consent of the other. Assignment of IBM rights to receive payments or assignment by IBM in conjunction with the sale of the portion of IBM's business that includes a service is not restricted.

f. This CSA applies to IBM and Client and their respective Enterprise companies who avail themselves of the CSA. The parties shall coordinate the activities of Enterprise companies under the Agreement. Enterprise companies include (i) companies within the same country that Client or IBM control (by owning greater than 50% of the voting shares), and (ii) any other entity that controls, is controlled by or is under common control with Client or IBM and has signed a participation agreement.

g. All notices under the Agreement must be in writing and sent to the business address specified for the Agreement, unless a party designates in writing a different address. The parties consent to the use of electronic means and facsimile transmissions for communications as a signed writing. Any reproduction of the Agreement made by reliable means is considered an original. The Agreement supersedes any course of dealing, discussions or representations between the parties.

h. No right or cause of action for any third party is created by the Agreement or any transaction under it. Neither party will bring a legal action arising out of or related to the Agreement more than two years after the cause of action arose. Neither party is responsible for failure to fulfill its non-monetary obligations due to causes beyond its control. Each party will allow the other reasonable opportunity to comply before it claims the other has not met its obligations. Where approval, acceptance, consent, access, cooperation or similar action by either party is required, such action will not be unreasonably delayed or withheld.

i. IBM may use personnel and resources in locations worldwide, including third party contractors and subprocessors to support the delivery of the Cloud Services. IBM may transfer Content, including personally identifiable information, across country borders. A list of countries where Content may be processed for a Cloud Service is available at www.ibm.com/cloud/datacenters or as described in the Attachment or TD. IBM is responsible for the obligations under the Agreement even if IBM uses a third party contractor or subprocessors unless otherwise set forth in a TD. IBM will require subprocessors with access to Content to maintain technical and organizational security measures that will enable IBM to meet its obligations for a Cloud Service. A current list of subprocessors and their roles will be provided upon request.

j. IBM may offer additional customization, configuration or other services to support Cloud Services, as detailed in a TD.

By______________________________________ Authorized signature	By______________________________________ Authorized signature
Title:	Title:
Name (type or print):	Name (type or print):
Date:	Date:
Client number:	Agreement number:
Enterprise number:	
Client address:	IBM address:

General Terms for Cloud Offerings

This General Terms for Cloud Offerings TOU provides additional terms applicable for IBM Cloud Services Client may order under either the International Passport Advantage Agreement or the International Passport Advantage Express Agreement, as applicable ("Base Agreement") and are in addition to other applicable Transaction Documents (TDs) and Attachments, collectively the complete agreement ("Agreement") regarding transactions for a Cloud Service.

1. Content and Data Protection

a. IBM's Data Security and Privacy Principles for IBM Cloud Services (DSP), at http://www.ibm.com/cloud/data-security, apply for generally available Cloud Service offerings. Specific security features and functions of a Cloud Service may be provided in an Attachment and TDs. Client is responsible to assess the suitability of each Cloud Service for Client's intended use and Content and to take necessary actions to order, enable, or use available data protection features appropriate for the Content being used with a Cloud Service. By using the Cloud Service, Client accepts responsibility for use of the Cloud Services, and acknowledges that it meets Client's requirements and processing instructions to enable compliance with applicable laws.

b. IBM will treat all Content as confidential by not disclosing Content except to IBM employees, contractors, and only to the extent necessary to deliver the Cloud Service.

c. IBM's Data Processing Addendum at http://www.ibm.com/dpa and applicable DPA Exhibit(s) apply to personal data contained in Content, if and to the extent: i) the European General Data Protection Regulation (EU/2016/679) (GDPR); or ii) other data protection laws identified at http://ibm.com/dpa/dpl apply.

d. IBM will return or remove Content from IBM computing resources upon the expiration or cancellation of the Cloud Service, or earlier upon Client's request. IBM may charge for certain activities performed at Client's request (such as delivering Content in a specific format). IBM does not archive Content, however some Content may remain in Cloud Service backup files until expiration of such files as governed by IBM's backup retention practices.

e. Upon request by either party, IBM, Client or affiliates of either, will enter into additional agreements as required by law in the prescribed form for the protection of personal or regulated personal data included in Content. The parties agree (and will ensure that of their respective affiliates) that such additional agreements will be subject to the terms of the Agreement.

2. Changes

a. Client acknowledges that IBM may modify: i) a Cloud Service; and ii) the DSP, from time to time at IBM's sole discretion and such modifications will replace prior versions as of the effective date. Updates to a TD (such as a service description or statement of work) will take effect upon a new order or for TDs previously agreed to by the Client will take effect upon the change effective date for ongoing services, or upon the renewal date for Cloud Services that automatically renew. The intent of any modification will be to i) improve or clarify existing commitments, ii) maintain alignment to current adopted standards and applicable laws, or iii) provide additional features and functionality. Modifications will not degrade the security or data protection features or functionality of a Cloud Service.

b. IBM may withdraw a Cloud Service on 12 months' notice and IBM will continue to provide the Cloud Service for the remainder of Client's unexpired term or work with Client to migrate to another IBM offering. Access to non-IBM services may be withdrawn at any time.

3. Payment and Taxes

a. Based on selected billing frequency, IBM will invoice Client the charges due at the beginning of the billing frequency term, except for overage and usage type of charges which will be invoiced in arrears. One time charges will be billed upon acceptance of an order.

b. If IBM has not otherwise committed to pricing during the term of a Cloud Service, then IBM may change charges on thirty days' notice.

4. Compliance with Laws

a. Each party is responsible for complying with: i) laws and regulations applicable to its business and Content; and ii) import, export and economic sanction laws and regulations, including defense trade control regime of any jurisdiction, including the International Traffic in Arms Regulations and those of the United States that prohibit or restrict the export, re-export, or transfer of products, technology, services or data, directly or indirectly, to or for certain countries, end uses or end users.

b. If Client or any user exports or imports Content or use of any portion of the Cloud Service outside the country of Client's business address, IBM will not serve as the exporter or importer, except as required by data protection laws.

5. Term and Termination

a. The term of a Cloud Service begins on the date IBM notifies Client that Client can access the Cloud Service. IBM will specify whether the Cloud Service renews automatically, proceeds on a continuous use basis, or terminates at the end of the term. For automatic renewal, unless Client provides written notice to IBM or the IBM Business Partner involved in the Cloud Service not to renew at least 30 days prior to the term expiration date, the Cloud Service will automatically renew for the specified term. For continuous use, the Cloud Service will continue to be available on a month to month basis until Client provides 30 days written notice to IBM or the IBM Business Partner involved in the Cloud Service of termination. The Cloud Service will remain available to the end of the calendar month after such 30 day period.

b. IBM may suspend or limit, to the extent necessary, Client's use of a Cloud Service if IBM determines there is a material breach of Client's obligations, a security breach, violation of law, or breach of the use terms, including prohibited uses, set forth in Base Agreement and section 7(g) below. If the cause of the suspension can reasonably be remedied, IBM will provide notice of the actions Client must take to reinstate the Cloud Service. If Client fails to take such actions within a reasonable time, IBM may terminate the Cloud Service. Failure to pay is a material breach.

c. Client may terminate a Cloud Service on one month's notice: i) at the written recommendation of a government or regulatory agency following a change in either applicable law or the Cloud Services; ii) if IBM's modification to the computing environment used to provide the Cloud Service causes Client to be noncompliant with applicable laws; or iii) if IBM notifies Client of a modification that has a material adverse effect on Client's use of the Cloud Service, provided that IBM will have 90 days to work with Client to minimize such effect. In the event of such termination, IBM shall refund a portion of any prepaid amounts for the applicable Cloud Service for the period after the date of termination. If a Cloud Service is terminated for any other reason, Client shall pay to IBM, on the date of termination, the total amounts due per the Cloud Service terms. Upon termination, IBM may assist Client in transitioning Client's Content to an alternative technology for an additional charge and under separately agreed terms.

6. Hybrid and Dual Entitlement Offerings

a. Hybrid and Dual Entitlement offerings are Cloud Services which provide Client with access to Programs for use in the environment of Client's choice as well as software as a service functions provided in an IBM cloud environment. Programs, Support, and Program updates are provided in accordance with the Agreement and the section titled "Programs and IBM Software Subscription and Support" of the IBM International Passport Advantage Agreement (Z125-5831-10) (or equivalent agreement in place between the parties), with the following modifications:

(1) Client's Program license ends when the Cloud Service subscription ends. Client agrees to promptly remove all such Programs from all Client selected computing environments and destroy all copies;

(2) any specified money back guarantee does not apply for identified Programs;

(3) for Hybrid Entitlement offerings, separate entitlements are required for the simultaneous use of the Cloud Service and use of the Programs in a Client computing environment; and

(4) for Dual Entitlement offerings, entitlements permit simultaneous use of the Cloud Services and use of the identified Programs in a Client computing environment.

7. General

a. IBM is as an information technology provider only. Any directions, suggested usage, or guidance provided by IBM or a Cloud Service does not constitute medical, clinical, legal, accounting, or other licensed professional advice. Client and its authorized users are responsible for the use of the Cloud Service within any professional practice and should obtain their own expert advice. Client is responsible for its use of IBM and Non-IBM products and services.

b. IBM may offer Non-IBM services, or an IBM Cloud Service may enable access to Non-IBM services, that may require acceptance of third party terms identified in the TD. Linking to or use of Non-IBM services constitutes Client's agreement with such terms. IBM is not a party to such third party agreements and is not responsible for such Non-IBM services.

c. Client may use enabling software only in connection with use of the Cloud Service and according to any licensing terms if specified in a TD. Enabling software is provided as-is, without warranties of any kind.

d. A Cloud Service or feature of a Cloud Service is considered "Preview" when IBM makes such services or features available at no charge, with limited or pre-release functionality, or for a limited time to try available functionality (such as beta, trial, no-charge, or preview designated Cloud Services). Preview services are excluded from available service level agreements. A Preview service may not be covered by support and IBM may change or discontinue a Preview service at any time and without notice. IBM is not obligated to release a Preview service or make an equivalent service generally available. Preview services are made available as-is, without warranties of any kind.

e. Account Data is information, other than Content and BCI, that Client provides to IBM to enable Client's use of a Cloud Service or that IBM collects using tracking technologies, such as cookies and web beacons, regarding Client's use of a Cloud Service. IBM, its affiliates, and contractors of either, may use Account Data, for example, to enable product features, administer use, personalize experience, and otherwise support or improve use of the Cloud Service. The IBM Privacy Statement at https://www.ibm.com/privacy/ (or equivalent country version) provides additional details with respect to Account Data and BCI as described in the Base Agreement.

f. IBM may use personnel and resources in locations worldwide, including contractors to support the delivery of the Cloud Services. IBM may transfer Content, including personal data, across country borders. A list of countries where Content may be processed for a Cloud Service offering is described in a TD. IBM is responsible for the obligations under the Agreement even if IBM uses a contractor and will have appropriate agreements in place to enable IBM to meet its obligations for a Cloud Service.

g. Client may not use Cloud Services if failure of the Cloud Service could lead to death, bodily injury, or property or environmental damage. Client may not: i) reverse engineer any portion of a Cloud Service; ii) assign or resell direct access to a Cloud Service to a third party outside Client's Enterprise; or iii) combine Cloud Services with Client's value add to create a commercially available Client branded solution that Client markets to its end user customers unless otherwise agreed.

h. IBM may offer additional customization, configuration or other services to support Cloud Services, as detailed in a TD.

8. Previous Base Agreement Versions

a. For Clients acquiring Cloud Services under a Base Agreement version prior to version 10 dated Nov 2017, IBM SaaS offerings are IBM Cloud Services and the following additional terms apply.

8.1 Content and Data Protection

a. Content consists of all data, software, and information that Client or its authorized users provides, authorizes access to, or inputs to the Cloud Service. Use of the Cloud Service will not affect Client's ownership or license rights in such Content. IBM, its affiliates, and contractors of either may access and use the Content solely for the purpose of providing and managing the Cloud Service.

b. Client is responsible for obtaining all necessary rights and permissions to enable, and grants such rights and permissions to, IBM, its affiliates, and contractors of either, to use, provide, store and otherwise process Content in the Cloud Service. This includes Client making necessary disclosures and obtaining consent, if required, before providing individuals' information, including personal or other regulated data in such Content. If any Content could be subject to governmental regulation or may require security measures beyond those specified by IBM for a Cloud Service, Client will not input, provide, or allow such Content unless specifically permitted in the terms of the relevant TD or unless IBM has otherwise first agreed in writing to implement additional security and other measures.

8.2 Warranty

a. IBM warrants that it provides Cloud Services using commercially reasonable care and skill in accordance with the applicable Attachment or SD. The warranty for a Cloud Service ends when the Cloud Service ends.

8.3 Scheduled Maintenance

a. Cloud Services are designed to be available 24/7, subject to maintenance. Client will be notified of scheduled maintenance.

Data Security and Privacy Principles for IBM Cloud Services

The technical and organizational measures provided in this Data Security and Privacy attachment (DSP) apply to IBM Cloud Services, including any underlying applications, platforms, and infrastructure components operated and managed by IBM in providing the Cloud Service (components), except where Client is responsible for security and privacy and otherwise specified in a transaction document (TD). Client is responsible for: a) determining whether the Cloud Service is suitable for Client's use and; b) implementing and managing security and privacy measures for elements not provided and managed by IBM within the Cloud Service described in applicable Attachments and TDs (such as systems and applications built or deployed by Client upon an Infrastructure as a Service offering, or Client end-user access control to Software as a Service offerings). The measures implemented and maintained by IBM within each Cloud Service will be subject to annual certification of compliance with ISO 27001 or SSAE SOC 2 or both.

1. Data Protection

a. Security and privacy measures for each Cloud Service are designed in accordance with IBM's secure engineering and privacy-by-design practices to protect Content input into a Cloud Service, and to maintain the availability of such Content pursuant to the Agreement, including applicable Attachments and TDs. Client is the sole controller for any personal data included in the Content and appoints IBM as a processor to process such personal data (as those terms are defined in Regulation (EU) 2016/679, General Data Protection Regulation). IBM will treat all Content as confidential by not disclosing Content except to IBM employees, contractors, and subprocessors, and only to the extent necessary to deliver the Cloud Service, unless otherwise specified in a TD.

b. IBM will securely sanitize physical media intended for reuse prior to such reuse, and will destroy physical media not intended for reuse, consistent with National Institute of Standards and Technology, United States Department of Commerce (NIST), guidelines for media sanitization.

c. Upon request, IBM will provide evidence of stated compliance and accreditation, such as certificates, attestations, or reports resulting from accredited independent third-party audits, such as ISO 27001, SSAE SOC 2, and other industry standards as specified in a TD. Where applicable, the accredited independent third-party audits will occur at the frequency required by the relevant standard to maintain the Cloud Service's stated compliance and accreditation.

d. Additional security and privacy information specific to a Cloud Service may be available in the relevant TD or other standard documentation to aide in Client's initial and ongoing assessment of a Cloud Service's suitability for use. Such information may include evidence of stated certifications and accreditations, information related to such certifications and accreditations, data sheets, FAQs, and other generally available documentation. IBM will direct Client to available standard documentation if asked to complete Client-preferred questionnaires or forms and Client agrees such documentation will be utilized in lieu of any such request. IBM may charge an additional fee to complete any Client-preferred questionnaires or forms or to provide consultation to Client for such purposes.

2. Security Policies

a. IBM will maintain and follow IT security policies and practices that are integral to IBM's business and mandatory for all IBM employees. The IBM CIO will maintain responsibility and executive oversight for such policies, including formal governance and revision management, employee education, and compliance enforcement.

b. IBM will review its IT security policies at least annually and amend such policies as IBM deems reasonable to maintain protection of Cloud Services and Content processed therein.

c. IBM will maintain and follow its standard mandatory employment verification requirements for all new hires and will extend such requirements to wholly owned IBM subsidiaries. In accordance with IBM internal process and procedures, these requirements will be periodically reviewed and include, but may not be limited to, criminal background checks, proof of identity validation, and additional checks as deemed necessary by IBM. Each IBM company is responsible for implementing these requirements in its hiring process as applicable and permitted under local law.

d. IBM employees will complete security and privacy education annually and certify each year that they will comply with IBM's ethical business conduct, confidentiality, and security policies, as set out in IBM's Business Conduct Guidelines. Additional policy and process training will be provided to persons granted administrative access to Cloud Service components that is specific to their role within IBM's operation and support of the Cloud Service, and as required to maintain compliance and certifications stated in the relevant TD.

3. Security Incidents

a. IBM will maintain and follow documented incident response policies consistent with NIST guidelines for computer security incident handling and will comply with data breach notification terms of the Agreement.

b. IBM will investigate unauthorized access and unauthorized use of Content of which IBM becomes aware (security incident), and, within the Cloud Service scope, IBM will define and execute an appropriate response plan. Client may notify IBM of a suspected vulnerability or incident by submitting a technical support request.

c. IBM will notify Client without undue delay upon confirmation of a security incident that is known or reasonably suspected by IBM to affect Client. IBM will provide Client with reasonably requested information about such security incident and the status of any IBM remediation and restoration activities.

4. **Physical Security and Entry Control**

   a. IBM will maintain appropriate physical entry controls, such as barriers, card-controlled entry points, surveillance cameras, and manned reception desks, to protect against unauthorized entry into IBM facilities used to host the Cloud Service (data centers). Auxiliary entry points into data centers, such as delivery areas and loading docks, will be controlled and isolated from computing resources.

   b. Access to data centers and controlled areas within data centers will be limited by job role and subject to authorized approval. Use of an access badge to enter a data center and controlled areas will be logged, and such logs will be retained for not less than one year. IBM will revoke access to controlled data center areas upon separation of an authorized employee. IBM will follow formal documented separation procedures that include, but are not limited to, prompt removal from access control lists and surrender of physical access badges.

   c. Any person duly granted temporary permission to enter a data center facility or a controlled area within a data center will be registered upon entering the premises, must provide proof of identity upon registration, and will be escorted by authorized personnel. Any temporary authorization to enter, including deliveries, will be scheduled in advance and require approval by authorized personnel.

   d. IBM will take precautions to protect the Cloud Service's physical infrastructure against environmental threats, both naturally occurring and man-made, such as excessive ambient temperature, fire, flood, humidity, theft, and vandalism.

5. **Access, Intervention, Transfer and Separation Control**

   a. IBM will maintain documented security architecture of networks managed by IBM in its operation of the Cloud Service. IBM will separately review such network architecture, including measures designed to prevent unauthorized network connections to systems, applications and network devices, for compliance with its secure segmentation, isolation, and defense-in-depth standards prior to implementation. IBM may use wireless networking technology in its maintenance and support of the Cloud Service and associated components. Such wireless networks, if any, will be encrypted and require secure authentication and will not provide direct access to Cloud Service networks. Cloud Service networks do not use wireless networking technology.

   b. IBM will maintain measures for a Cloud Service that are designed to logically separate and prevent Content from being exposed to or accessed by unauthorized persons. IBM will maintain appropriate isolation of its production and non-production environments, and, if Content is transferred to a non-production environment, for example in order to reproduce an error at Client's request, security and privacy protections in the non-production environment will be equivalent to those in production.

   c. To the extent described in the relevant TD, IBM will encrypt Content not intended for public or unauthenticated viewing when transferring Content over public networks and enable use of a cryptographic protocol, such as HTTPS, SFTP, and FTPS, for Client's secure transfer of Content to and from the Cloud Service over public networks.

   d. IBM will encrypt Content at rest when specified in a TD. If the Cloud Service includes management of cryptographic keys, IBM will maintain documented procedures for secure key generation, issuance, distribution, storage, rotation, revocation, recovery, backup, destruction, access, and use.

   e. If IBM requires access to Content, it will restrict such access to the minimum level required. Such access, including administrative access to any underlying components (privileged access), will be individual, role-based, and subject to approval and regular validation by authorized IBM personnel following the principles of segregation of duties. IBM will maintain measures to identify and remove redundant and dormant accounts with privileged access and will promptly revoke such access upon the account owner's separation or the request of authorized IBM personnel, such as the account owner's manager.

   f. Consistent with industry standard practices, and to the extent natively supported by each component managed by IBM within the Cloud Service, IBM will maintain technical measures enforcing timeout of inactive sessions, lockout of accounts after multiple sequential failed login attempts, strong password or passphrase authentication, and measures requiring secure transfer and storage of such passwords and passphrases.

   g. IBM will monitor use of privileged access and maintain security information and event management measures designed to: a) identify unauthorized access and activity; b) facilitate a timely and appropriate response; and c) enable internal and independent third-party audits of compliance with documented IBM policy.

   h. Logs in which privileged access and activity are recorded will be retained in compliance with IBM's worldwide records management plan. IBM will maintain measures designed to protect against unauthorized access, modification, and accidental or deliberate destruction of such logs.

   i. To the extent supported by native device or operating system functionality, IBM will maintain computing protections for its end-user systems that include, but may not be limited to, endpoint firewalls, full disk encryption, signature-based malware detection and removal, time-based screen locks, and endpoint management solutions that enforce security configuration and patching requirements.

6. **Service Integrity and Availability Control**

   a. IBM will: a) perform security and privacy risk assessments of its Cloud Services at least annually; b) perform penetration testing and vulnerability assessments, including automated system and application security scanning and manual ethical hacking, before production release and annually thereafter; c) enlist a qualified independent third-party to perform penetration testing at least annually; d) perform automated management and routine verification of underlying components' compliance with security configuration requirements; and e) remediate identified vulnerabilities or noncompliance with its security configuration requirements based on associated risk, exploitability, and impact. IBM will take reasonable steps to avoid Cloud Service disruption when performing its tests, assessments, scans, and execution of remediation activities.

b. IBM will maintain policies and procedures designed to manage risks associated with the application of changes to its Cloud Services. Prior to implementation, changes to a Cloud Service, including its systems, networks, and underlying components, will be documented in a registered change request that includes a description and reason for the change, implementation details and schedule, a risk statement addressing impact to the Cloud Service and its clients, expected outcome, rollback plan, and documented approval by authorized personnel.

c. IBM will maintain an inventory of all information technology assets used in its operation of the Cloud Service. IBM will continuously monitor and manage the health, including capacity, and availability of the Cloud Service and underlying components.

d. Each Cloud Service will be separately assessed for business continuity and disaster recovery requirements pursuant to documented risk management guidelines. Each IBM Cloud Service will have, to the extent warranted by such risk assessment, separately defined, documented, maintained, and annually validated business continuity and disaster recovery plans consistent with industry standard practices. Recovery point and time objectives for the Cloud Service, if provided, will be established with consideration given to the Cloud Service's architecture and intended use, and will be described in the relevant TD. Physical media intended for off-site storage, if any, such as media containing Cloud Service backup files, will be encrypted prior to transport.

e. IBM will maintain measures designed to assess, test, and apply security advisory patches to the Cloud Service and its associated systems, networks, applications, and underlying components within the Cloud Service scope. Upon determining that a security advisory patch is applicable and appropriate, IBM will implement the patch pursuant to documented severity and risk assessment guidelines. Implementation of security advisory patches will be subject to IBM change management policy.

Data Processing Addendum

This Data Processing Addendum (DPA) and its applicable DPA Exhibits apply to the Processing of Personal Data by IBM on behalf of Client (Client Personal Data) subject to the General Data Protection Regulation 2016/679 (GDPR) or any other data protection laws identified at http://www.ibm.com/dpa/dpl (together 'Data Protection Laws') in order to provide services (Services) pursuant to the Agreement between Client and IBM. DPA Exhibits for each Service will be provided in the applicable Transaction Document (TD). This DPA is incorporated into the Agreement. Capitalized terms used and not defined herein have the meanings given them in the applicable Data Protection Laws. In the event of conflict, the DPA Exhibit prevails over the DPA which prevails over the rest of the Agreement.

1. Processing

1.1 Client is: (a) a Controller of Client Personal Data; or (b) acting as Processor on behalf of other Controllers and has been instructed by and obtained the authorization of the relevant Controller(s) to agree to the Processing of Client Personal Data by IBM as Client's subprocessor as set out in this DPA. Client appoints IBM as Processor to Process Client Personal Data. If there are other Controllers, Client will identify and inform IBM of any such other Controllers prior to providing their Personal Data, in accordance with the DPA Exhibit.

1.2 A list of categories of Data Subjects, types of Client Personal Data, Special Categories of Personal Data and the processing activities is set out in the applicable DPA Exhibit for a Service. The duration of the Processing corresponds to the duration of the Service, unless otherwise stated in the DPA Exhibit. The purpose and subject matter of the Processing is the provision of the Service as described in the Agreement.

1.3 IBM will Process Client Personal Data according to Client's documented instructions. The scope of Client's instructions for the Processing of Client Personal Data is defined by the Agreement, and, if applicable, Client's and its authorized users' use and configuration of the features of the Service. Client may provide further legally required instructions regarding the Processing of Client Personal Data (Additional Instructions) as described in Section 10.2. If IBM notifies Client that an Additional Instruction is not feasible, the parties shall work together to find an alternative. If IBM notifies the Client that neither the Additional Instruction nor an alternative is feasible, Client may terminate the affected Service, in accordance with any applicable terms of the Agreement. If IBM believes an instruction violates the Data Protection Laws, IBM will immediately inform Client, and may suspend the performance of such instruction until Client has modified or confirmed its lawfulness in documented form.

1.4 Client shall serve as a single point of contact for IBM. As other Controllers may have certain direct rights against IBM, Client undertakes to exercise all such rights on their behalf and to obtain all necessary permissions from the other Controllers. IBM shall be discharged of its obligation to inform or notify another Controller when IBM has provided such information or notice to Client. Similarly, IBM will serve as a single point of contact for Client with respect to its obligations as a Processor under this DPA.

1.5 IBM will comply with all Data Protection Laws in respect of the Services applicable to IBM as Processor. IBM is not responsible for determining the requirements of laws or regulations applicable to Client's business, or that a Service meets the requirements of any such applicable laws or regulations. As between the parties, Client is responsible for the lawfulness of the Processing of the Client Personal Data. Client will not use the Services in a manner that would violate applicable Data Protection Laws.

2. Technical and organizational measures

2.1 Client and IBM agree that IBM will implement and maintain the technical and organizational measures set forth in the applicable DPA Exhibit (TOMs) which ensure a level of security appropriate to the risk for IBM's scope of responsibility. TOMs are subject to technical progress and further development. Accordingly, IBM reserves the right to modify the TOMs provided that the functionality and security of the Services are not degraded.

3. Data Subject Rights and Requests

3.1 IBM will inform Client of requests from Data Subjects exercising their Data Subject rights (e.g., including but not limited to rectification, deletion and blocking of data) addressed directly to IBM regarding Client Personal Data. Client shall be responsible to handle such requests of Data Subjects. IBM will reasonably assist Client in handling such Data Subject requests in accordance with Section 10.2.

3.2 If a Data Subject brings a claim directly against IBM for a violation of their Data Subject rights, Client will reimburse IBM for any cost, charge, damages, expenses or loss arising from such a claim, to the extent that IBM has notified Client about the claim and given Client the opportunity to cooperate with IBM in the defense and settlement of the claim. Subject to the terms of the Agreement, Client may claim from IBM damages resulting from Data Subject claims for a violation of their Data Subject rights caused by IBM's breach of its obligations under this DPA and the respective DPA Exhibit.

4. Third Party Requests and Confidentiality

4.1 IBM will not disclose Client Personal Data to any third party, unless authorized by the Client or required by law. If a government or Supervisory Authority demands access to Client Personal Data, IBM will notify Client prior to disclosure, unless such notification is prohibited by law.

4.2 IBM requires all of its personnel authorized to Process Client Personal Data to commit themselves to confidentiality and not Process such Client Personal Data for any other purposes, except on instructions from Client or unless required by applicable law.

5. Audit

5.1 IBM shall allow for, and contribute to, audits, including inspections, conducted by the Client or another auditor mandated by the Client in accordance with the following procedures:

a. Upon Client's written request, IBM will provide Client or its mandated auditor with the most recent certifications and/or summary audit report(s), which IBM has procured to regularly test, assess and evaluate the effectiveness of the TOMs, to the extent set out in the DPA Exhibit.

b. IBM will reasonably cooperate with Client by providing available additional information concerning the TOMs, to help Client better understand such TOMs.

c. If further information is needed by Client to comply with its own or other Controllers audit obligations or a competent Supervisory Authority's request, Client will inform IBM in writing to enable IBM to provide such information or to grant access to it.

d. To the extent it is not possible to otherwise satisfy an audit right mandated by applicable law or expressly agreed by the Parties, only legally mandated entities (such as a governmental regulatory agency having oversight of Client's operations), the Client or its mandated auditor may conduct an onsite visit of the IBM facilities used to provide the Service, during normal business hours and only in a manner that causes minimal disruption to IBM's business, subject to coordinating the timing of such visit and in accordance with any audit procedures described in the DPA Exhibit in order to reduce any risk to IBM's other customers.

Any other auditor mandated by the Client shall not be a direct competitor of IBM with regard to the Services and shall be bound to an obligation of confidentiality.

5.2 Each party will bear its own costs in respect of paragraphs a. and b. of Section 5.1, otherwise Section 10.2 applies accordingly.

6. Return or Deletion of Client Personal Data

6.1 Upon termination or expiration of the Agreement IBM will either delete or return Client Personal Data in its possession as set out in the respective DPA Exhibit, unless otherwise required by applicable law.

7. Subprocessors

7.1 Client authorizes the engagement of other Processors to Process Client Personal Data (Subprocessors). A list of the current Subprocessors is set out in the respective DPA Exhibit. IBM will notify Client in advance of any addition or replacement of the Subprocessors as set out in the respective DPA Exhibit. Within 30 days after IBM's notification of the intended change, Client can object to the addition of a Subprocessor on the basis that such addition would cause Client to violate applicable legal requirements. Client's objection shall be in writing and include Client's specific reasons for its objection and options to mitigate, if any. If Client does not object within such period, the respective Subprocessor may be commissioned to Process Client Personal Data. IBM shall impose substantially similar but no less protective data protection obligations as set out in this DPA on any approved Subprocessor prior to the Subprocessor initiating any Processing of Client Personal Data.

7.2 If Client legitimately objects to the addition of a Subprocessor and IBM cannot reasonably accommodate Client's objection, IBM will notify Client. Client may terminate the affected Services as set out inthe

Agreement, otherwise the parties shall cooperate to find a feasible solution in accordance with the dispute resolution process.

8. Transborder Data Processing

8.1 In the case of a transfer of Client Personal Data to a country not providing an adequate level of protection pursuant to the Data Protection Laws (Non-Adequate Country), the parties shall cooperate to ensure compliance with the applicable Data Protection Laws as set out in the following Sections. If Client believes the measures set out below are not sufficient to satisfy the legal requirements, Client shall notify IBM and the parties shall work together to find an alternative.

8.2 By entering into the Agreement, Client is entering into EU Standard Contractual Clauses as set out in the applicable DPA Exhibit (EU SCC) with (i) each Subprocessor listed in the respective DPA Exhibit that is an IBM affiliate located in a Non-Adequate Country (IBM Data Importers) and (ii) IBM, if located in a Non-Adequate Country, as follows:

a. if Client is a Controller of all or part of the Client Personal Data, Client is entering into the EU SCC in respect to such Client Personal Data; and

b. if Client is acting as Processor on behalf of other Controllers of all or part of the Client Personal Data, then Client is entering into the EU SCC:

(i) as back-to-back EU SCC in accordance with Clause 11 of the EU Standard Contractual Clauses (Back-to-Back SCC), provided that Client has entered into separate EU Standard Contractual Clauses with the Controllers; or

(ii) on behalf of the other Controller(s).

Client agrees in advance that any new IBM Data Importer engaged by IBM in accordance with Section 7 shall become an additional data importer under the EU SCC and/or Back-to-Back SCC.

8.3 If a Subprocessor located in a Non-Adequate Country is not an IBM Data Importer (Third Party Data Importer) and EU SCC are entered into in accordance with Section 8.2, then, IBM or an IBM Data Importer shall enter into Back-to-Back SCC with such a Third Party Data Importer. Otherwise, Client on its own behalf and/or, if required, on behalf of other Controllers shall enter into separate EU Standard Contractual Clauses or Back-to-Back SCC as provided by IBM.

8.4 If Client is unable to agree to the EU SCC or Back-to-Back SCC on behalf of another Controller, as set out in section 8.2 and 8.3, Client will procure the agreement of such other Controller to enter into those agreements directly. Additionally, Client agrees and, if applicable, procures the agreement of other Controllers that the EU SCC or the Back-to-Back SCC, including any claims arising from them, are subject to the terms set forth in the Agreement, including the exclusions and limitations of liability. In case of conflict, the EU SCC and Back-to-Back SCC shall prevail.

9. Personal Data Breach

9.1 IBM will notifyClient without undue delay after becoming aware of a Personal Data Breach with respect to the Services. IBM will promptly investigate the Personal Data Breach if it occurred on IBM infrastructure or in another area IBM is responsible for and will assist Client as set out in Section 10.

10. Assistance

10.1 IBM will assist Client by technical and organizational measures for the fulfillment of Client's obligation to comply with the rights of Data Subjects and in ensuring compliance with Clients obligations relating to the security of Processing, the notification and communication of a Personal Data Breach and the Data Protection Impact Assessment, including prior consultation with the responsible Supervisory Authority, if required, taking into account the nature of the processing and the information available to IBM.

10.2 Client will make a written request for any assistance referred to in this DPA. IBM may charge Client no more than a reasonable charge to perform such assistance or an Additional Instruction, such charges to be set forth in a quote and agreed in writing by the parties, or as set forth in an applicable change control provision of the Agreement. If Client does not agree to the quote, the parties agree to reasonably cooperate to find a feasible solution in accordance with the dispute resolution process.