Data Protection Addendum (DPA)

This Data Protection Addendum ("**DPA**") forms part of, amends and supplements the Core Terms, and/or any other written agreement entered into between the Customer and LabVantage that covers the use of the Offerings, as applicable (the "**Agreement**") and will apply to the extent that LabVantage or a LabVantage Affiliate (collectively "**Provider**") processes Personal Data on Customer's behalf pursuant to the Agreement.

Capitalized terms not defined in this DPA are defined in the Agreement or in the applicable Data Protection Laws.

1. Definitions.

1.1. "**Controller**" means the natural or legal person, public authority, agency, or other body which, alone or jointly with others, determines the purposes and means of Processing of Personal Data.

1.2. "**Customer Personal Data**" means Personal Data in Customer Content.

1.3. "**Data Protection Laws**" means all laws and regulations applicable to the Processing of Customer Personal Data under the Agreement, including, as applicable: (i) the California Consumer Privacy Act, as amended by the California Privacy Rights Act, and any binding regulations promulgated thereunder ("**CCPA**"), (ii) the General Data Protection Regulation (Regulation (EU) 2016/679) ("**EU GDPR**" or "**GDPR**"), (iii) the Swiss Federal Act on Data Protection ("**FADP**"), (iv) the EU GDPR as it forms part of the law of England and Wales by virtue of section 3 of the European Union (Withdrawal) Act 2018 (the "**UK GDPR**") and (v) the UK Data Protection Act 2018; in each case, as updated, amended or replaced from time to time.

1.4. "**Data Subject**" means the identified or identifiable natural person to whom Customer Personal Data relates.

1.5. "**EEA**" means European Economic Area.

1.6 "**LabVantage Affiliate**" means any entity owned directly or indirectly by LabVantage's parent, LabVantage Systems Ltd. (UK).

1.6. "**Personal Data**" means information about an identified or identifiable natural person, or which otherwise constitutes "personal data," "personal information," "personally identifiable information" or similar terms as defined in Data Protection Laws.

1.7. "**Processing**" means any operation or set of operations that is performed on Personal Data such as collection, recording, organization, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure, or destruction.

1.8. "**Processor**" means a natural or legal person, public authority, agency, or other body which Processes Personal Data on behalf of the Controller.

1.9. "**Restricted Transfer**" means: (i) where EU GDPR applies, a transfer of Customer Personal Data from the EEA to a country outside the EEA that is not subject to an adequacy determination, (ii) where UK GDPR applies, a transfer of Customer Personal Data from the United Kingdom to any other country that is not subject to an adequacy determination or (iii) where FADP applies, a transfer of Customer Personal Data from Switzerland to any other country that is not subject to an adequacy determination.

1.10. “**Security Incident**” means any breach of security that leads to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, Customer Personal Data being Processed by Provider.

1.11. “**Subprocessor**” means any third party authorized by Provider to Process any Customer Personal Data.

1.12. “**Subprocessor List**” means the list of Provider’s Subprocessors as identified or linked to on the DPA Setup Page.

2. Scope and Duration.

2.1. **Roles of the Parties**. For purposes of this DPA, LabVantage and/or any LabVantage Affiliate (collectively “Provider”) will be a Processor of Customer Personal Data. Customer will be the Controller or Processor of Customer Personal Data.

2.2. **Scope of DPA**. This DPA applies to Provider’s Processing of Customer Personal Data under the Agreement to the extent such Processing is subject to Data Protection Laws. This DPA is governed by the governing law of the Agreement unless otherwise required by Data Protection Laws.

2.3. **Term and Termination**. The Term and Termination section of the Agreement also apply to this DPA.

2.4. **Order of Precedence**. In the event of any conflict or inconsistency among the following documents, the order of precedence will be: (1) any Standard Contractual Clauses or other measures to which the parties have agreed in Schedule 2 (Cross-Border Transfer Mechanisms) or Schedule 3 (Region-Specific Terms), (2) this DPA and (3) the Agreement. To the fullest extent permitted by Data Protection Laws, any claims brought in connection with this DPA (including its Schedules) will be subject to the terms and conditions, including, but not limited to, the exclusions and limitations, set forth in the Agreement.

3. Processing of Personal Data.

3.1. **Customer Instructions**.

(a) Provider will Process Customer Personal Data as a Processor only: (i) in accordance with Customer Instructions or (ii) to comply with Provider’s obligations under applicable laws, subject to any notice requirements under Data Protection Laws.

(b) “Customer Instructions” means: (i) Processing to provide the Cloud Service and perform Provider’s obligations in the Agreement (including this DPA) and (ii) other reasonable documented instructions of Customer consistent with the terms of the Agreement.

(c) Details regarding the Processing of Customer Personal Data by Provider are set forth in Schedule 1 (Subject Matter and Details of Processing)

Provider will notify Customer if it receives an instruction that Provider reasonably determines infringes Data Protection Laws (but Provider has no obligation to actively monitor Customer’s compliance with Data Protection Laws).

3.2. **Confidentiality.** (a) Provider will protect Customer Personal Data in accordance with its confidentiality obligations as set forth in the Agreement. (b) Provider will ensure personnel who Process Customer Personal Data either enter into written confidentiality agreements or be bound by confidentiality policies as a condition of their employment.

3.3. **Compliance with Laws**.

(i) Provider and Customer will each comply with Data Protection Laws in their respective Processing of Customer Personal Data.

(ii) Customer will comply with Data Protection Laws in its issuing of Customer Instructions to Provider. Customer will ensure that it has established all necessary lawful bases under Data Protection Laws to enable Provider to lawfully Process Customer Personal Data for the purposes contemplated by the Agreement (including this DPA), including, as applicable, by obtaining all necessary consents from, and giving all necessary notices to, Data Subjects.

3.4. **Changes to Laws.** The parties will work together in good faith to negotiate an amendment to this DPA as either party reasonably considers necessary to address the requirements of Data Protection Laws from time to time.

4. **Subprocessors.**

4.1. **Use of Subprocessors.**

(i) Customer authorizes Provider to engage Subprocessors to Process Customer Personal Data. Customer further agrees that Provider may engage its Affiliates as Subprocessors. Provider will: (a) enter into a written agreement with each Subprocessor imposing data Processing and protection obligations substantially the same as those set out in this DPA and (b) remain liable for compliance with the obligations of this DPA and for any acts or omissions of a Subprocessor that cause Provider to breach any of its obligations under this DPA.

(ii) Provider will maintain an up-to-date list of its Subprocessors, including their functions and locations, as specified in the Schedule 3 ("Subprocessor List").

4.2. **Notice of New Subprocessors.** Provider may update the Subprocessor List from time to time.

5. Security.

5.1. **Security Measures.** Provider will implement and maintain reasonable and appropriate technical and organizational measures, procedures and practices, as appropriate to the nature of the Customer Personal Data, that are designed to protect the security, confidentiality, integrity and availability of Customer Personal Data and protect against Security Incidents, in accordance with Provider's Security Measures referenced in the Agreement and as further described at https://www.labvantage.com/legal/security ("**Security Measures**"). Provider will regularly monitor its compliance with its Security Measures.

5.2. **Incident Notice and Response**. (a) Provider will implement and follow procedures to detect and respond to Security Incidents. (b) Provider will: (i) notify Customer without undue delay and, in any event, not later than 72 hours, after becoming aware of a Security Incident affecting Customer and (ii) make reasonable efforts to identify the cause of the Security Incident, mitigate the effects, and remediate the cause to the extent within Provider's reasonable control. (c) Upon Customer's request and taking into account the nature of the applicable Processing, Provider will assist Customer by providing, when available, information reasonably necessary for Customer to meet its Security Incident notification obligations under Data Protection Laws, including information needed for Customer to report the Security Incident to a Supervisory Authority.

(d) Customer shall determine if the Security Incident needs to be reported to the appropriate Supervisory Authority and shall be responsible for such reporting.

(e) Customer acknowledges that Provider's notification of a Security Incident is not an acknowledgement by Provider of its fault or liability.

(f) Security Incidents do not include unsuccessful attempts or activities that do not compromise the security of Customer Personal Data, including unsuccessful login attempts, pings, port scans, denial of service attacks or other network attacks on firewalls or networked systems.

5.3**. Customer Responsibilities.**

(i) Customer is responsible for reviewing the information made available by Provider relating to data security and making an independent determination as to whether the Cloud Service meets Customer's requirements and legal obligations under Data Protection Laws.

(ii) Customer is solely responsible for complying with Security Incident notification laws applicable to Customer and fulfilling any obligations to give notices to government authorities, affected individuals or others relating to any Security Incidents.

6. Data Protection Impact Assessment.

Upon Customer's request and taking into account the nature of the applicable Processing, to the extent such information is available to Provider, Provider will assist Customer in fulfilling Customer's obligations under Data Protection Laws to carry out a data protection impact or similar risk assessment related to Customer's use of the Cloud Service, including, if required by Data Protection Laws, by assisting Customer in consultations with relevant government authorities.

7. Data Subject Requests.

7.1. **Assisting Customer.** Upon Customer's request and taking into account the nature of the applicable Processing, Provider will assist Customer by appropriate technical and organizational measures, insofar as possible, in complying with Customer's obligations under Data Protection Laws to respond to requests from individuals to exercise their rights under Data Protection Laws, provided that Customer cannot reasonably fulfill such requests independently (including through use of the Cloud Service).

7.2. **Data Subject Requests.** If Provider receives a request from a Data Subject in relation to the Data Subject's Customer Personal Data, Provider will notify Customer and advise the Data Subject to submit the request to Customer (but not otherwise communicate with the Data Subject regarding the request except as may be required by Data Protection Laws), and Customer will be responsible for responding to any such request.

8. Data Return or Deletion.

(i) Following termination or expiration of the Agreement, Provider will, in accordance with its obligations under the Agreement, delete all Customer Personal Data from Provider's systems.

(ii) Deletion will be in accordance with industry-standard secure deletion practices. Provider will issue a certificate of deletion upon Customer's request.

(iii) Notwithstanding the foregoing, Provider may retain Customer Personal Data: (a) as required by Data Protection Laws or (b) in accordance with its standard backup or record retention policies, provided that, in either case, Provider will (x) maintain the confidentiality of, and otherwise comply with the applicable provisions of this DPA with respect to, retained Customer Personal Data and (y) not further Process retained Customer Personal Data except for such purpose(s) and duration specified in such applicable Data Protection Laws. (z) where possible, shall anonymize the data to protect confidentiality. For example: data in audit trails that cannot be deleted.

9. Audits.

9.1. **Provider Records Generally**. Provider will keep records of its Processing in compliance with Data Protection Laws and, upon Customer's request but no more than once every two (2) years, make available to Customer any records reasonably necessary to demonstrate compliance with Provider's obligations under this DPA and Data Protection Laws.

9.2. **Third-Party Compliance Program**. (a) Provider will describe its third-party audit and certification programs (if any) and make executive summary copies of its audit reports (each, an "Audit Report")

available to Customer upon Customer's written request at reasonable intervals (subject to confidentiality obligations).

(b) Customer may share a copy of Audit Reports with relevant government authorities as required upon their request.

(c) Customer agrees that any audit rights granted by Data Protection Laws will be satisfied by Audit Reports and the procedures of Section 9.3 (Customer Audit) below.

(d) Customer agrees that such Audit Reports are LabVantage confidential documentation and shall not share or distribute these reports, or post them to media, to anyone outside of the Customer.

9.3. **Customer Audit.**

(a) Subject to the terms of this Section 9.3, Customer has the right, at Customer's expense, to conduct an audit of reasonable scope and duration pursuant to a mutually agreed-upon audit plan with Provider that is consistent with the Audit Parameters (an "Audit"). (b) Customer may exercise its Audit right: (i) to the extent Provider's provision of an Audit Report does not provide sufficient information for Customer to verify Provider's compliance with this DPA or the parties' compliance with Data Protection Laws, (ii) as necessary for Customer to respond to a government authority audit or (iii) in connection with a Security Incident.

(c) Each Audit must conform to the following parameters ("Audit Parameters"):

(i) be conducted by Customer representative(s), or an independent third party hired by Customer at their expense, that will enter into a confidentiality agreement with Provider,

(ii) be limited in scope to matters reasonably required for Customer to assess Provider's compliance with this DPA and the parties' compliance with Data Protection Laws, (iii) occur at a mutually agreed date and time and only during Provider's regular business Eastern Time Zone hours (New Jersey, USA),

(iv) audit duration shall not exceed one day (8 hours) for routine periodic audits, with the possibility of extending to a two (2) day (sixteen (16) hour)) for an initial audit,

(v) occur no more than once every two (2) years (unless required under Data Protection Laws or in connection with a Security Incident),

(vi) shall be conducted virtually using conferencing media,

(vii) cover only facilities controlled by Provider, (viii) restrict findings to Customer Personal Data only and

(viii) treat any results as confidential information to the fullest extent permitted by Data Protection Laws.

10. Cross-Border Transfers/Region-Specific Terms.

10.1. Cross-Border Data Transfers

(a) Provider (and its Affiliates) may Process and transfer Customer Personal Data globally as necessary to perform LabVantage's obligation under the Agreement.

(ii) If Provider engages in a Restricted Transfer, it will comply with Schedule 3 (Cross-Border Transfer Mechanisms).

10.2. Region-Specific Terms. To the extent that Provider Processes Customer Personal Data protected by Data Protection Laws in one of the regions listed in Schedule 3 (Region-Specific Terms), the applicable sections of Schedule 3 will apply in addition to the terms of this DPA.

11. Limitation of Liability.

The total liability of each Party (and their respective employees, directors, officers, affiliates, successors, and assigns) to the other, arising out of or related to this DPA, whether in contract, tort, or other theory of liability, will not, when taken together in the aggregate, exceed the limitation of liability set forth in the Agreement. This section is not intended to modify or limit the parties' joint and several liability for Data Subject claims under GDPR Article 82 or the right of contribution under GDPR Article 82. Further, this section is not intended to limit either party's responsibility to pay penalties imposed on that party by a regulatory authority for that party's violation of applicable Data Protection Laws.

12 Term.

This term of this DPA will be coextensive with the term of the Agreement. Each Party's obligations under this DPA will terminate upon expiration or termination of the Agreement, unless otherwise mandated under applicable law, otherwise agreed by the Parties in writing, or otherwise provided in the EU Standard Contractual Clauses.

13. Miscellaneous.

This DPA supersedes and replaces any existing data processing addendum that the Parties may have previously entered into in connection with the Offerings and all prior and contemporaneous agreements, oral and written, regarding the subject matter of this DPA between LabVantage and Customer. The Customer acknowledges and agrees that LabVantage may update this DPA from time to time in case required as a result of (i) changes in Data Protection Laws; (ii) the release of new Offerings and/or features thereof or material changes thereto; (iii) when the changes: (a) are commercially reasonable; (b) do not result in a material reduction in the level of security provided by LabVantage for Personal Data (c) do not expand the scope of, or remove any restrictions on, LabVantage Processing of Personal Data as set forth in this DPA; and (d) do not otherwise have a material adverse impact on Customer's rights under this DPA. Except as provided by this DPA, the Agreement remains unchanged and in full force and effect. This DPA will be governed by and construed in accordance with governing law and jurisdiction provisions in the Services Agreement, except where otherwise indicated by the EU Standard Contractual clauses or Data Protection Laws.

Schedule 1

Subject Matter and Details of Processing

Data Importer / Processor:

#1 Data Importer Company: (Processor)	LabVantage Solutions, Inc.
Address:	Headquarters: 265 Davidson Ave, Suite 220, Somerset, NJ, 08873, USA
Contact name, position, email, phone	**For data privacy issues:** Donald DiPalma, Director of Quality and Data Protection Officer Email: ddipalma@labvantage.com or Quality@labvantage.com Phone: 908-333-0192 **Software support issues:** Carla Vandra, Director of Customer Support Email: cvandra@labvantage.com or Support@labvantage.com Phone: 908-333-0185 or 877-477-5467 **Software implementation support issues:** Software implementation support is to be identified in the Statement of Work (SOW). LabVantage contact details are to detemined at the time of project kickoff and identifed in the project documenation.
Activities relevant to the data transferred under these Clauses:	**Software support:** Provide product support service for issues related to the LabVantage software not operating as intended (bugs), for enhancement requests, and to allow customers to download software. **Software implementaion support:** Provide software implemenation services to evaluate customer requirements, configure and customize the application to meet the customer needs and requirements as defined in the Statement of Work.

Description of Transfer / Processing:

Categories of data subjects whose personal data is transferred	**Software Support:** A select few Customer employees and / or customer representatives. These are identified and controlled by the Customer. **Software implementation support:** A select few Customer employee and / or customer representatives that are invovled in the project. These are identified and controlled by the Customer.
Categories of personal data transferred	Business contact information that includes: contact name, username, email address, phone number, and role.
Sensitive data transferred (if applicable) and applied restrictions or safeguards that fully take into consideration the nature of the data and the risks involved, such as for instance strict purpose limitation, access restrictions (including access only for staff having followed specialised training), keeping a record of access to the data, restrictions for onward transfers or additional security measures.	No sensitive personal data is transferred or retained.

The frequency of the transfer (e.g., whether the data is transferred on a one-off or continuous basis).	**Software Support:** • Once for the creation of the data subject user account in the VantageCare Customer Portal. • Ongoing as part of an active Master Software Services Agreement. **Software implementation support:** • Once for the creation of the data subject user account in the JIRA-PSO application used for project management. • Ongoing as part of an active SOW and project.
Nature of the processing	Collection, storage, data management (creation, edition, deletion), anonymization, retrieval, disclosure
Purpose(s) of the data transfer and further processing	**Software Support:** Provide product support service for issues related to our software not operating as intended (bugs), for enhancement requests, and to allow customers to download software. These are captured in VantageCare. **Software implementation support:** Provide software implemenation services to evaluate customer requirements, configure and customize the application to meet the customer needs and requirements as defined in the Statement of Work.
The period for which the personal data will be retained, or, if that is not possible, the criteria used to determine that period	**Software Support:** • Personal contact information stored in VantageCare will be retained for the period of time the person has access to VantageCare and until the person requests the account to be closed / terminated. • Support information will be retained in VantageCare indefinitely for historical purposes. If requested, LabVantage will anonymize personal data residing in VantageCare. **Software implementation support:** • Personal contact information, stored in the JIRA-PSO application, will be retained for the period of time the person has access to JIRA-PSO and until the person requests the account to be closed / terminated. • Project information will be retained in JIRA-PSO for the duration of the active project plus 2 years after the close of the project. If requested, LabVantage will anonymize personal data residing in JIRA-PSO.
For transfers to (sub-) processors, also specify subject matter, nature, and duration of the processing	Transfer to Amazon Web Services (AWS) sub-processor is only for the use of their cloud infrastructure hosting services for VantageCare that is used to track product issues and customers may download software. The retention period is the same as that for the VantageCare Customer Portal.

Schedule 2 Cross-Border Transfer Mechanisms

1. **Definitions**. Capitalized terms not defined in this Schedule are defined in the DPA.
   1.1. "**EU Standard Contractual Clauses**" or "**EU SCCs**" means the Standard Contractual Clauses approved by the European Commission in decision 2021/914 or any subsequent update enacted by the European Commission.
   1.2. "**UK International Data Transfer Agreement**" means the International Data Transfer Addendum to the EU Commission Standard Contractual Clauses issued by the UK Information Commissioner, Version B1.0, in force as of March 21, 2022.
   1.3. In addition:

"**Designated EU Governing Law**" means:	The law of the EU country where Customer is located. If Customer is not located in the EU, then the Designated EU Governing Law will mean Cyprus.
"**Designated EU Member State**" means:	The law of the EU country where Customer is located. If Customer is not located in the EU, then the Designated EU Member State will mean Cyprus.

2. **EU Transfers**. Where Customer Personal Data is protected by EU GDPR and is subject to a Restricted Transfer, the following applies:
   2.1. The EU SCCs are hereby incorporated by reference as follows:
      (a) Module 2 (Controller to Processor) applies where Customer is a Controller of Customer Personal Data and Provider is a Processor of Customer Personal Data;
      (b) Module 3 (Processor to Processor) applies where Customer is a Processor of Customer Personal Data (on behalf of a third-party Controller) and Provider is a Processor of Customer Personal Data;
      (c) Customer is the "data exporter" and Provider is the "data importer"; and
      (d) By entering into this DPA, each party is deemed to have signed the EU SCCs (including their Annexes) as of the DPA Effective Date.
   2.2. For each Module, where applicable the following applies:
      (a) the optional docking clause in Clause 7 does not apply;
      (b) in Clause 9, Option 2 will apply, the minimum time period for prior notice of Subprocessor changes shall be as set out in Section 4.3 of this DPA, and Provider shall fulfill its notification obligations by notifying Customer of any Subprocessor changes in accordance with Section 4.3 of this DPA;
      (c) in Clause 11, the optional language does not apply;
      (d) in Clause 13, all square brackets are removed with the text remaining;
      (e) in Clause 17, Option 1 will apply, and the EU SCCs will be governed by Designated EU Governing Law;
      (f) in Clause 18(b), disputes will be resolved before the courts of the Designated EU Member State;
      (g) Schedule 1 (Subject Matter and Details of Processing) to this DPA contains the information required in Annex 1 of the EU SCCs; and
      (h) Schedule 2 (Technical and Organizational Measures) to this DPA contains the information required in Annex 2 of the EU SCCs.
   2.3. Where context permits and requires, any reference in this DPA to the EU SCCs shall be read as a reference to the EU SCCs as modified in the manner set forth in this Section 2.

3. **Swiss Transfers**. Where Customer Personal Data is protected by the FADP and is subject to a Restricted Transfer, the following applies:
   3.1. The EU SCCs apply as set forth in Section 2 (EU Transfers) of this Schedule 3 with the following modifications:
      (a) in Clause 13, the competent supervisory authority shall be the Swiss Federal Data Protection and Information Commissioner;
      (b) in Clause 17 (Option 1), the EU SCCs will be governed by the laws of Switzerland;
      (c) in Clause 18(b), disputes will be resolved before the courts of Switzerland;
      (d) the term Member State must not be interpreted in such a way as to exclude Data Subjects in Switzerland from enforcing their rights in their place of habitual residence in accordance with Clause 18(c); and
      (e) All references to the EU GDPR in this DPA are also deemed to refer to the FADP.

4. **UK Transfers**. Where Customer Personal Data is protected by the UK GDPR and is subject to a Restricted Transfer, the following applies:
   4.1. The EU SCCs apply as set forth in Section 2 (EU Transfers) of this Schedule 3 with the following modifications:
      (a) each party shall be deemed to have signed the "UK Addendum to the EU Standard Contractual Clauses" ("**UK Addendum**") issued by the Information Commissioner's Office under section 119 (A) of the Data Protection Act 2018;
      (b) the EU SCCs shall be deemed amended as specified by the UK Addendum in respect of the transfer of Customer Personal Data;
      (c) in Table 1 of the UK Addendum, the parties' key contact information is located in Schedule 1 (Subject Matter and Details of Processing) to this DPA;
      (d) in Table 2 of the UK Addendum, information about the version of the EU SCCs, modules, and selected clauses which this UK Addendum is appended to are located above in this Schedule 3;
      (e) in Table 3 of the UK Addendum:
         (i) the list of parties is located in Schedule 1 (Subject Matter and Details of Processing) to this DPA;
         (ii) The description of transfer is located in Schedule 1 (Subject Matter and Details of Processing) to this DPA;
         (iii) Annex II is located in Schedule 2 (Technical and Organizational Measures) to this DPA; and
         (iv) The list of Subprocessors is located in Schedule 1 (Subject Matter and Details of Processing) to this DPA.
      (f) in Table 4 of the UK Addendum, both the Importer and the Exporter may end the UK Addendum in accordance with its terms (and the respective box for each is deemed checked); and
      (g) in Part 2: Part 2 - Mandatory Clauses of the Approved Addendum, being the template Addendum B.1.0 issued by the ICO and laid before Parliament in accordance with section 119 (A) of the Data Protection Act 2018 on 2 February 2022, as it is revised under section 18 of those Mandatory Clauses.

Schedule 3

List of Subprocessors:

Sub-Processor Name:	Amazon Web Services (AWS)
Address:	Corporate address: 410 Terry Avenue North, Seattle, WA, 98109, United States Data Center: Virginia, USA Exact street and town location are omitted for security purposes
Contact person's name, position, and contact details:	Mike Thomsen Title: Director of Technical Services Email: mthomsen@labvantage.com Phone: 908-333-0176
Description of processing (including a clear delimitation of responsibilities in case several sub-processors are authorized):	AWS hosts the VantageCare Customer Portal system where product issues are reported by the customer, for software / bug tracking / resolution and software can be downloaded. AWS is also the hosting provider for any Cloud Offerings purchased by Customer.