AMENDMENT SEVEN
TO
PARTICIPATING ADDENDUM
NASPO ValuePoint COOPERATIVE PURCHASING PROGRAM
Cloud Solution Products and Services
Administered by the State of Utah

MASTER AGREEMENT
Master Agreement No: AR2472
Carahsoft Technology Corporation
And
State of Oklahoma by and through the Office of Management and Enterprise Services

(Oklahoma Contract No.: SW1022C)

This Seventh Amendment ("Amendment") to the Participating Addendum is entered into effective as of October 6, 2023 ("Effective Date"), by and between the State of Oklahoma by and through the Office of Management and Enterprise Services ("State") and Carahsoft Technology Corporation ("Vendor").

For good and valuable consideration, the parties agree as follows:

1) **The parties agree the following attachments are incorporated hereto:**

   Attachment A: Information Security Terms; and

   Attachment B: UiPath EULA Terms.

Attachment A and B will supplement the terms and conditions of Oklahoma Contract No.: SW1022C with the inclusion of mutually agreed to terms between the State, Vendor, and UiPath, Inc.

Participating Entity: State of Oklahoma by and through the **Office of Management and Enterprise Services**	Contractor: **Carahsoft Technology Corporation**
Signature: Michael Toland	Signature: Jack Blumenthal
Name: Michael Toland	Name: Jack Blumenthal
Title: CISO	Title: Team Lead
Date: 10/09/2023	Date: 10/9/2023

Information Security Requirements

1. **General Information Security Requirements**
   a. No employee of Contractor or its subcontractors will be granted access to State of Oklahoma agency information systems without the prior completion and approval of applicable logon authorization and acceptable use requests.
   b. Contractor or its subcontractors will notify applicable State of Oklahoma agencies when employees who have access to agency information systems are terminated.
   c. Contractor or its subcontractors will disclose to Client any suspected breach of the security of the information system or the data contained therein in the most expedient time possible and without unreasonable delay and will cooperate with Client during the investigation of any such incident.
   d. Contractor or its subcontractors agree to adhere to the State of Oklahoma "Information Security Policy, Procedures, and Guidelines" available at: https://oklahoma.gov/content/dam/ok/en/omes/documents/InfoSecPPG.pdf

2. **HIPAA Requirements**
   a. Contractor shall agree to use and disclose Protected Health Information in compliance with the Standards for Privacy of Individually Identifiable Health Information (Privacy Rule) (45 C.F.R. Parts 160 and 164) under the Health Insurance Portability and Accountability Act (HIPAA) of 1996. The definitions set forth in the Privacy Rule are incorporated by reference into this Contract (45 C.F.R. §§ 160.103 and 164.501).
   b. If applicable, Contractor will sign and adhere to a Business Associate Agreement (BAA). The Business Associate Agreement provides for satisfactory assurances that Contractor will use the information only for the purposes for which it was engaged. Contractor agrees it will safeguard the information from misuse, and will comply with HIPAA as it pertains to the duties stated within the contract. Failure to comply with the requirements of this standard may result in funding being withheld from Contractor, and/or full audit and inspection of Contractor's security compliance as it pertains to this contract.
   c. Business Associate Terms Definitions:
      i. Unless otherwise defined in this BAA, all capitalized terms used in this BAA have the meanings ascribed in the HIPAA Regulations, provided; however, that "PHI" and "ePHI" shall mean Protected Health Information and Electronic Protected Health Information, respectively, as defined in 45 C.F.R. § 160.103, limited to the information Business Associate received from or created or received on behalf of the applicable State of Oklahoma agency as a Business Associate. "Administrative Safeguards" shall have the same meaning as the term "administrative safeguards in 45 C.F.R. § 164.304, with the exception that it shall apply to the management of the conduct of Business Associate's workforce, not the State of Oklahoma agency workforce, in relation to the protection of that information.

ii. Business Associate. "Business Associate" shall generally have the same meaning as the term "Business Associate" at 45 C.F.R. 160.103, and in reference to the party to this agreement, shall mean the entity whose name appears below.
iii. Covered Entity. "Covered Entity" shall generally have the same meaning as the term "Covered Entity" at 45 C.F.R. 160.103.
iv. HIPAA Rules. "HIPAA Rules" shall mean the Privacy, Security, Breach Notification, and Enforcement Rules at 45 C.F.R. Part 160 and Part 164, all as may be amended.
v. The following terms used in this Agreement shall have the same meaning as those terms in the HIPAA Rules: Breach, Data Aggregation, Designated Record Set, Disclosure, Health Care Operations, Individual, Minimum Necessary, Notice of Privacy Practices, Protected Health Information, required by law, Secretary, Security Incident, Sub-Contractor, Unsecured PHI, and Use.

d. Obligations of Business Associate: Business Associate may use Electronic PHI and PHI (collectively, "PHI") solely to perform its duties and responsibilities under this Agreement and only as provided in this Agreement. Business Associate acknowledges and agrees that PHI is confidential and shall not be used or disclosed, in whole or in part, except as provided in this Agreement or as required by law. Specifically, Business Associate agrees it will:
   i. use or further disclose PHI only as permitted in this Agreement or as Required by Law, including, but not limited to the Privacy and Security Rule;
   ii. use appropriate safeguards, and comply with Subpart C of 45 C.F.R. Part 164 with respect to Electronic PHI, to prevent use or disclosure of PHI other than as provided for by this Agreement;
   iii. implement and document appropriate administrative, physical, and technical safeguards to protect the confidentiality, integrity, and availability of PHI that it creates, receives, maintains, or transmits for or on behalf of Covered Entity in accordance with 45 C.F.R. 164;
   iv. implement and document administrative safeguards to prevent, detect, contain, and correct security violations in accordance with 45 C.F.R. 164;
   v. make its policies and procedures required by the Security Rule available to Covered Entity solely for purposes of verifying BA's compliance and the Secretary of the Department of Health and Human Services (HHS);
   vi. not receive remuneration from a third party in exchange for disclosing PHI received from or on behalf of Covered Entity;
   vii. in accordance with 45 C.F.R. 164.502(e)(1) and 164.308(b), if applicable, require that any Sub-Contractors that create, receive, maintain or transmit PHI on behalf of the Business Associate agree to the same restrictions, conditions, and requirements that apply to the Business Associate with respect to such information; this shall be in the form of a written HIPAA Business Associate Contract and a fully executed copy will be provided to the Contract Monitor;
   viii. report to Covered Entity in writing any use or disclosure of PHI that is not permitted under this Agreement as soon as reasonably practicable but in no event later than five

calendar days from becoming aware of it and mitigate, to the extent practicable and in cooperation with Covered Entity, any harmful effects known to it of a use or disclosure made in violation of this Agreement;

ix. promptly report to Covered Entity in writing and without unreasonable delay and in no case later than five calendar days any successful Security Incident, as defined in the Security Rule, with respect to Electronic PHI;

x. with the exception of law enforcement delays that satisfy the requirements of 45 C.F.R. 164.412, notify Covered Entity promptly, in writing and without unreasonable delay and in no case later than five calendar days, upon the discovery of a breach of Unsecured PHI. Such notice shall include, to the extent possible, the name of each individual who's Unsecured PHI has been, or is reasonably believed by Business Associate to have been, accessed, acquired, or disclosed during such Breach. Business Associate shall also, to the extent possible, furnish Covered Entity with any other available information that Covered Entity is required to include in its notification to Individuals under 45 C.F.R. § 164.404(c) at the time of Business Associate's notification to Covered Entity or promptly thereafter as such information becomes available. As used in this Section, "breach" shall have the meaning given such term at 45 C.F.R. 164.402;

xi. to the extent allowed by law, indemnify and hold Covered Entity harmless from all claims, liabilities costs, and damages arising out of or in any manner related to the disclosure by Business Associate of any PHI or to the breach by Business Associate of any obligation related to PHI;

xii. provide access to PHI it maintains in a Designated Record Set to Covered Entity, or if directed by Covered Entity to an Individual in order to meet the requirements of 45 C.F.R. 164.524. In the event that any Individual requests access to PHI directly from Business Associate, Business Associate shall forward such request to Covered Entity within five working days of receiving a request. This shall be in the form of a written HIPAA Business Associate Contract and a fully executed copy will be provided to the Contract Monitor. Any denials of access to the PHI requested shall be the responsibility of Covered Entity;

xiii. make PHI it maintains in a Designated Record Set available to Covered Entity for amendment and incorporate any amendments to PHI in accordance with 45 C.F.R. 164.526;

xiv. document disclosure of PHI it maintains in a Designated Record Set and information related to such disclosure as would be required for Covered Entity to respond to a request by an Individual for an accounting of disclosures of PHI, in accordance with 45 C.F.R. 164.528, and within five working days of receiving a request from Covered Entity, make such disclosure documentation and information available to Covered Entity. In the event the request for an accounting is delivered directly to Business Associate, Business Associate shall forward within five working days of receiving a request such request to Covered Entity;

xv. make its internal practices, books, and records related to the use and disclosure of PHI received from or created or received by Business Associate on behalf of Covered Entity available to the Secretary of the Department of HHS, authorized governmental officials, and Covered entity for the purpose of determining Business Associate's compliance with the Privacy Rule. Business Associate shall give Covered Entity advance written notice of requests from HHS or government officials and provide Covered Entity with a copy of all documents made available; and

xvi. require that all of its Sub-Contractors, vendors, and agents to whom it provides PHI or who create, receive, use, disclose, maintain, or have access to Covered Entity's PHI shall agree in writing to requirements, restrictions, and conditions at least as stringent as those that apply to Business Associate under this Agreement, including but not limited to implementing reasonable and appropriate safeguards to protect PHI, and shall require that its Sub-Contractors, vendors, and agents agree to indemnify and hold harmless Covered Entity for their failure to comply with each of the provisions of this Agreement.

e. Permitted Uses and Disclosures of PHI by Business Associate: Except as otherwise provided in this Agreement, Business Associate may use or disclose PHI on behalf of or to provide services to Covered Entity for the purposes specified in this Agreement, if such use or disclosure of PHI would not violate the Privacy Rule if done by Covered Entity. Unless otherwise limited herein, Business Associate may:
   i. use PHI for its proper management and administration or to fulfill any present or future legal responsibilities of Business Associate;
   ii. disclose PHI for its proper management and administration or to fulfill any present or future legal responsibilities of Business Associate, provided that; (i) the disclosures required by law; or (ii) Business Associate obtains reasonable assurances from any person to whom the PHI is disclosed that such PHI will be kept confidential and will be used or further disclosed only as Required by Law or for the purpose(s) for which it was disclosed to the person, and the person commits to notifying Business Associate of any instances of which it is aware in which the confidentiality of the PHI has been breached;
   iii. disclose PHI to report violations of law to appropriate federal and state authorities; or
   iv. aggregate the PHI with other data in its possession for purposes of Covered Entity's Health Care Operations;
   v. make uses and disclosures and requests for protected health information consistent with Covered Entity's minimum necessary policies and procedures;
   vi. de-identify any and all PHI obtained by Business Associate under this BAA, and use such de-identified data, all in accordance with the de-identification requirements of the Privacy Rule [45 C.F.R. § (d)(1)].

f. Obligations of Covered Entity
   i. Covered Entity shall notify Business Associate of any changes in, or revocation of, the permission by an individual to use or disclose his or her PHI, to the extent that such changes may affect Business Associate's use or disclosure of PHI.

ii. Covered Entity shall notify Business Associate of any restriction on the use or disclosure of PHI that Covered Entity has agreed to or is required to abide by under 45 C.F.R. 164.522, to the extent that such restriction may affect Business Associate's use or disclosure of protected health information.

iii. Covered Entity shall not request Business Associate use or disclose PHI in any manner that would violate the Privacy Rule if done by Covered Entity.

iv. Covered Entity agrees to timely notify Business Associate, in writing, of any arrangements between Covered Entity and the Individual that is the subject of PHI that may impact in any manner the use and/or disclosure of the PHI by Business Associate under this BAA.

g. Term and Termination:

i. Obligations of Business Associate upon Termination. Upon termination of this Agreement for any reason, Business Associate, with respect to PHI received from Covered Entity, or created, maintained, or received by Business Associate on behalf of Covered Entity, shall:

(1) retain only that PHI that is necessary for Business Associate to continue its proper management and administration or to carry out its legal responsibilities;

(2) return to Covered Entity (or, if agreed to by Covered Entity, destroy) the remaining PHI that the Business Associate still maintains in any form;

(3) continue to use appropriate safeguards and comply with Subpart C of 45 C.F.R. Part 164 with respect to PHI to prevent use or disclosure of the PHI, other than as provided for in this Section, for as long as Business Associate retains the PHI;

(4) not use or disclose the PHI retained by Business Associate other than for the purposes for which such PHI was retained and subject to the same conditions set out at above under "Permitted Uses and Disclosures By Business Associate" that applied prior to termination; and

(5) return to Covered Entity (or, if agreed to by Covered Entity, destroy) the PHI retained by Business Associate when it is no longer needed by Business Associate for its proper management and administration or to carry out its legal responsibilities.

ii. All other obligations of Business Associate under this Agreement shall survive termination.

iii. Should the applicable State of Oklahoma agency become aware of a pattern of activity or practice that constitutes a material breach of a material term of this BAA by Business Associate, the agency shall provide Business Associate with written notice of such a breach in sufficient detail to enable Contractor to understand the specific nature of the breach. The Client shall be entitled to terminate the Underlying Contract associated with such breach if, after the applicable State of Oklahoma agency provides the notice to Business Associate, Business Associate fails to cure the breach within a reasonable time period not less than thirty (30) days specified in such notice; provided, however, that such time period specified shall be based on the nature of the breach involved per 45 C.F.R. §§ 164.504(e)(1)(ii)(A),(B) & 164.314 (a)(2)(i)(D).

h. Miscellaneous Provisions:
   i. No Third Party Beneficiaries: Nothing in this Agreement shall confer upon any person other than the parties and their respective successors or assigns, any rights, remedies, obligations, or liabilities whatsoever.
   ii. Business Associate recognizes that any material breach of this Business Associate Terms section or breach of confidentiality or misuse of PHI may result in the termination of this Agreement and/or legal action. Said termination may be immediate and need not comply with any termination provision in the parties' underlying agreement, if any.
   iii. The parties agree to amend this Agreement from time to time as is necessary for Covered Entity or Business Associate to comply with the requirements of the Privacy Rule and related laws and regulations.
   iv. The applicable State of Oklahoma agency shall make available its Notice of Privacy Practices.
   v. Any ambiguity in this Agreement shall be resolved in a manner that causes this Agreement to comply with HIPAA.
   vi. If Business Associate maintains a designated record set in an electronic format on behalf of Covered Entity, then Business Associate agrees that within 30 calendar days of expiration or termination of the parties' agreement, Business Associate shall provide to Covered Entity a complete report of all disclosures of and access to the designated record set covering the three years immediately preceding the termination or expiration. The report shall include patient name, date and time of disclosures/access, description of what was disclosed/accessed, purpose of disclosure/access, name of individual who received or accessed the information, and, if available, what action was taken within the designated record set.
   vii. Amendment: To the extent that any relevant provision of the HIPAA Regulations is materially amended in a manner that changes the obligations of Business Associates or Covered Entities, the Parties agree to negotiate in good faith appropriate amendment(s) to this Agreement to give effect to these revised obligations. The parties agree to amend this Agreement from time to time as is necessary for Covered Entity or to comply with the requirements of the Privacy Rule and related laws and regulations.

3. 42 C.F.R. Part 2 Related Provisions

a. Confidentiality of Information. Contractor's employees and agents shall have access to private data to the extent necessary to carry out the responsibilities, limited by the terms of this Agreement. Contractor accepts the responsibilities for providing adequate supervision and training to their employees and agents to ensure compliance with relevant confidentiality, privacy laws, regulations and contractual provisions. No private or confidential data collected, maintained, or used shall be disseminated except as authorized by statute and by terms of this Agreement, whether during the period of the Agreement or thereafter. Furthermore, Contractor:

i. Acknowledges that in receiving, transmitting, transporting, storing, processing, or otherwise dealing with any information received pursuant to this agreement that identifies or otherwise relates to the individuals under the care of or in the custody of a State of Oklahoma agency, it is fully bound by the provisions of the federal regulations governing the confidentiality of Alcohol and Drug Abuse Patient Records, 42 C.F.R. Part 2 and the HIPAA, 45 C.F.R. 45 Parts 142, 160, and 164, Title 43 A § 1-109 of Oklahoma Statutes, and may not use or disclose the information except as permitted or required by this Agreement or by law;

ii. Acknowledges that pursuant to 43A O.S. §1-109, all mental health and drug or alcohol treatment information and all communications between physician or psychotherapist and patient are both privileged and confidential and that such information is available only to persons actively engaged in treatment of the client or consumer or in related administrative work. Contractor agrees that such protected information shall not be available or accessible to staff in general and shall not be used for punishment or prosecution of an kind;

iii. Agrees to resist any efforts in judicial proceedings to obtain access to the protected information except as expressly provided for in the regulations governing the Confidentiality of Alcohol and Drug Abuse Patient Records, 42 C.F.R. Part 2;

iv. Agrees to use appropriate administrative, physical, and technical safeguards that reasonably and appropriately protect the confidentiality, integrity, and availability of the electronic protected health information that it creates, receives, maintains, or transmits on behalf of the State of Oklahoma agency and to use appropriate safeguards to prevent the unauthorized use or disclosure of the protected health information, and agrees that protected information will not be placed in the Child Protective Services (CPS) record of any individual involved with the Oklahoma Department of Human Services (DHS).

v. Agrees to report to the State of Oklahoma agency any use or disclosure or any security incident involving protected information not provided for by this Agreement. Such a report shall be made immediately when an employee becomes aware of such a disclosure, use, or security incident.

vi. Agrees to provide access to the protected information at the request of the State of Oklahoma agency or to an authorized individual as directed by the State of Oklahoma agency, in order to meet the requirement of 45 C.F.R. §164.524 which provides clients with the right to access and copy their own protected information;

vii. Agrees to make any amendments to the protected information as directed or agreed to by the State of Oklahoma agency, pursuant to 45 C.F.R. §164.526;

viii. Agrees to make available its internal practices, books, and records, including policies and procedures, relating to the use and disclosure of protected information received from the State of Oklahoma agency or created or received by the Contractor on behalf of the State of Oklahoma agency, to the State of Oklahoma agency and to the Secretary of the Department of Health and Human Services for purpose of the Secretary determining the giving party's compliance with HIPAA;

ix. Agrees to provide the State of Oklahoma agency, or an authorized individual, information to permit the State of Oklahoma agency to respond to a request by an individual for an accounting of disclosures in accordance with 45 C.F.R. §164.528.

b. Data Security. The Contractor agrees to maintain the data in a secure manner compatible with the content and use. The Contractor will control access to the data in compliance with the terms of this Agreement. Only the Contractor's personnel whose duties require the use of such information, will have regular access to the data. The Contractor's employees will be allowed access to the data only for the purpose set forth in this Agreement.

c. Data Destruction. Contractor agrees to follow State of Oklahoma agency policies regarding secure data destruction.

d. Use of Information. Contractor agrees that the information received or accessed through this Agreement shall not be used to the detriment of any individual nor for any purpose other than those stated in this Agreement.

e. Redisclosure of Data. The Contractor agrees not to redisclose any information to a third party not covered by the Agreement unless written permission by the State of Oklahoma agency is received and redisclosure is permitted under applicable law.

4. Federal Tax Information Requirements IRS Publication 1075

a. PERFORMANCE: In performance of this contract, the Contractor agrees to comply with and assume responsibility for compliance by officers or employees with the following requirements:

i. All work will be performed under the supervision of the contractor.

ii. The contractor and contractor's officers or employees to be authorized access to FTI must meet background check requirements defined in IRS Publication 1075. The contractor will maintain a list of officers or employees authorized access to FTI. Such list will be provided to the agency and, upon request, to the IRS.

iii. FTI in hardcopy or electronic format shall be used only for the purpose of carrying out the provisions of this contract. FTI in any format shall be treated as confidential and shall not be divulged or made known in any manner to any person except as may be necessary in the performance of this contract. Inspection or disclosure of FTI to anyone other than the contractor or the contractor's officers or employees authorized is prohibited.

iv. FTI will be accounted for upon receipt and properly stored before, during, and after processing. In addition, any related output and products require the same level of protection as required for the source material.

v. The contractor will certify that FTI processed during the performance of this contract will be completely purged from all physical and electronic data storage with no output to be retained by the contractor at the time the work is completed. If immediate purging of physical and electronic data storage is not possible, the contractor will certify that any FTI in physical or electronic storage will remain safeguarded to prevent unauthorized disclosures.

vi. Any spoilage or any intermediate hard copy printout that may result during the processing of FTI will be given to the agency. When this is not possible, the contractor will be responsible for the destruction of the spoilage or any intermediate hard copy printouts and will provide the agency with a statement containing the date of destruction, description of material destroyed, and the destruction method.

vii. All computer systems receiving, processing, storing, or transmitting FTI must meet the requirements in IRS Publication 1075. To meet functional and assurance requirements, the security features of the environment must provide for the managerial, operational, and technical controls. All security features must be available and activated to protect against unauthorized use of and access to FTI.

viii. No work involving FTI furnished under this contract will be subcontracted without the prior written approval of the IRS.

ix. Contractor will ensure that the terms of FTI safeguards described herein are included, without modification, in any approved subcontract for work involving FTI.

x. To the extent the terms, provisions, duties, requirements, and obligations of this contract apply to performing services with FTI, the contractor shall assume toward the subcontractor all obligations, duties and responsibilities that the agency under this contract assumes toward the contractor, and the subcontractor shall assume toward the contractor all the same obligations, duties and responsibilities which the contractor assumes toward the agency under this contract.

xi. In addition to the subcontractor's obligations and duties under an approved subcontract, the terms and conditions of this contract apply to the subcontractor, and the subcontractor is bound and obligated to the contractor hereunder by the same terms and conditions by which the contractor is bound and obligated to the agency under this contract.

xii. For purposes of this contract, the term "contractor" includes any officer or employee of the contractor with access to or who uses FTI, and the term "subcontractor" includes any officer or employee of the subcontractor with access to or who uses FTI.

xiii. The agency will have the right to void the contract if the contractor fails to meet the terms of FTI safeguards described herein.

b. CRIMINAL/CIVIL SANCTIONS

i. Each officer or employee of a contractor to whom FTI is or may be disclosed shall be notified in writing that FTI disclosed to such officer or employee can be used only for a purpose and to the extent authorized herein, and that further disclosure of any FTI for a purpose not authorized herein constitutes a felony punishable upon conviction by a fine of as much as $5,000 or imprisonment for as long as 5 years, or both, together with the costs of prosecution.

ii. Each officer or employee of a contractor to whom FTI is or may be accessible shall be notified in writing that FTI accessible to such officer or employee may be accessed only for a purpose and to the extent authorized herein, and that access/inspection of FTI without an official need-to-know for a purpose not authorized herein constitutes a criminal misdemeanor punishable upon conviction by a fine of as much as $1,000 or imprisonment for as long as 1 year, or both, together with the costs of prosecution.

iii. Each officer or employee of a contractor to whom FTI is or may be disclosed shall be notified in writing that any such unauthorized access, inspection or disclosure of FTI may also result in an award of civil damages against the officer or employee in an amount equal to the sum of the greater of $1,000 for each unauthorized access, inspection, or disclosure, or the sum of actual damages sustained as a result of such unauthorized access, inspection, or disclosure, plus in the case of a willful unauthorized access, inspection, or disclosure or an unauthorized access/inspection or disclosure which is the result of gross negligence, punitive damages, plus the cost of the action. These penalties are prescribed by IRC sections 7213, 7213A and 7431 and set forth at 26 CFR 301.6103(n)-1.

iv. Additionally, it is incumbent upon the contractor to inform its officers and employees of the penalties for improper disclosure imposed by the Privacy Act of 1974, 5 U.S.C. 552a. Specifically, 5 U.S.C. 552a(i)(1), which is made applicable to contractors by 5 U.S.C. 552a(m)(1), provides that any officer or employee of a contractor, who by virtue of his/her employment or official position, has possession of or access to agency records which contain individually identifiable information, the disclosure of which is prohibited by the Privacy Act or regulations established thereunder, and who knowing that disclosure of the specific material is so prohibited, willfully discloses the material in any manner to any person or agency not entitled to receive it, shall be guilty of a misdemeanor and fined not more than $5,000.

v. Granting a contractor access to FTI must be preceded by certifying that each officer or employee understands the agency's security policy and procedures for safeguarding FTI. A contractor and each officer or employee must maintain their authorization to access FTI through annual recertification of their understanding of the agency's security policy and procedures for safeguarding FTI. The initial certification and recertifications must be documented and placed in the agency's files for review. As part of the certification and at least annually afterwards, a contractor and each officer or employee must be advised of the provisions of IRC sections 7213, 7213A, and 7431 (see IRS Publication 1075, Exhibit 4, Sanctions for Unauthorized Disclosure, and IRS Publication 1075, Exhibit 5, Civil Damages for Unauthorized Disclosure). The training on the agency's security policy and procedures provided before the initial certification and annually thereafter must also cover the incident response policy and procedure for reporting unauthorized disclosures and data breaches. For the initial certification and the annual recertifications, the contractor and each officer or employee must sign, either with ink or electronic signature, a confidentiality statement certifying their understanding of the security requirements.

c. INSPECTION: The IRS and the Agency, with 24 hour notice, shall have the right to send its inspectors into the offices and plants of the contractor to inspect facilities and operations performing any work with FTI under this contract for compliance with requirements defined in IRS Publication 1075. The IRS' right of inspection shall include the use of manual and/or automated scanning tools to perform compliance and vulnerability assessments of information technology (IT) assets that access, store, process or transmit FTI. Based on the inspection, corrective actions may be required in cases where the contractor is found to be noncompliant with FTI safeguard requirements.

5. SSA Requirements (If applicable)

a. PERFORMANCE: In performance of this contract, the contractor agrees to comply with and assume responsibility for compliance by his or her employees with the following requirements:

i. All work will be done under the supervision of the contractor or the contractor's employees.

ii. Any SSA provided information made available shall be used only for carrying out the provisions of this Agreement. Information contained in such material shall be treated as confidential and shall not be divulged or made known in any manner to any person except as may be necessary in the performance of this contract. Inspection by or disclosure to anyone other than an officer or employee of the Contractor is prohibited.

iii. All SSA provided information shall be accounted for upon receipt and properly stored before, during, and after processing. In addition, all related output and products will be given the same level of protection as required for the source material.

iv. No work involving SSA provided information furnished under this contract shall be subcontracted without prior written approval by the applicable State of Oklahoma agency and the SSA.

v. The Contractor shall maintain a list of employees authorized access. Such list shall be provided upon request to the applicable State of Oklahoma agency or the SSA.

vi. Contractor or agents may not legally process, transmit, or store SSA-provided information in a cloud environment without explicit permission from SSA's Chief Information Officer. Proof of this authorization shall be provided to the Contractor by the applicable State of Oklahoma agency prior to accessing SSA provided information.

vii. Contractor shall provide security awareness training to all employees, contractors, and agents who access SSA-provided information. The training should be annual, mandatory, and certified by the personnel who receive the training. Contractor is also required to certify that each employee, contractor, and agent who views SSA-provided information certify that they understand the potential criminal, civil, and administrative sanctions or penalties for unlawful assess and/or disclosure.

viii. Contractor shall require employees, contractors, and agents to sign a non-disclosure agreement, attest to their receipt of Security Awareness Training, and acknowledge the rules of behavior concerning proper use and security in systems that process SSA-provided information. Contractor shall retain non-disclosure attestations for at least five (5) to seven (7) years for each employee who processes, views, or encounters SSA-provided information as part of their duties.

ix. The applicable State of Oklahoma agency shall provide the Contractor a copy of the SSA exchange agreement and all related attachments before initial disclosure of SSA data. Contractor is required to follow the terms of the applicable State of Oklahoma agency's data exchange agreement with the SSA. Prior to signing this Agreement, and thereafter at SSA's request, the applicable State of Oklahoma agency shall obtain from

the Contractor a current list of the employees of such Contractor with access to SSA data and provide such list to the SSA.

x. Where the Contractor processes, handles, or transmits information provided to the applicable State of Oklahoma agency by SSA or has authority to perform on the agency's behalf, the applicable State of Oklahoma agency shall clearly state the specific roles and functions of the Contractor within the Agreement.

xi. SSA requires all parties subject to this Agreement to exercise due diligence to avoid hindering legal actions, warrants, subpoenas, court actions, court judgments, state or Federal investigations, and SSA special inquiries for matters pertaining to SSA-provided information.

xii. SSA requires all parties subject to this Agreement to agree that any Client-owned or subcontracted facility involved in the receipt, processing, storage, or disposal of SSA-provided information operate as a "de facto" extension of the Client and is subject to onsite inspection and review by the Client or SSA with prior notice.

xiii. If the Contractor must send a computer, hard drive, or other computing or storage device offsite for repair, the Contractor must have a non-disclosure clause in their contract with the vendor. If the Contractor used the item in a business process that involved SSA-provided information and the vendor will retrieve or may view SSA-provided information during servicing, SSA reserves the right to inspect the Contractor's vendor contract. The Contractor must remove SSA-provided information from electronic devices before sending it to an external vendor for service. SSA expects the Contractor to render SSA-provided information unrecoverable or destroy the electronic device if they do not need to recover the information. The same applies to excessed, donated, or sold equipment placed into the custody of another organization.

xiv. In the event of a suspected or verified data breach involving SSA provided information, the Contractor shall notify the Client immediately.

xv. The Client shall have the right to void the contract if the contractor fails to provide the safeguards described above.

b. CRIMINAL/CIVIL SANCTIONS: The Act specifically provides civil remedies, 5 U.S.C. Sec. 552a(g), including damages, and criminal penalties, 5 U.S.C. Sec. 552a(i), for violations of the Act. The civil action provisions are premised violations of the Act committed by parties subject to this Agreement or regulations promulgated thereunder. An individual claiming such a violation by parties subject to this Agreement may bring civil action in a federal district court. If the individual substantially prevails, the court may assess reasonable attorney fees and other litigation costs. In addition, the court may direct the parties subject to this Agreement to grant the plaintiff access to his/her records, and when appropriate direct an amendment or correction of records subject to the Act. Actual damages may be awarded to the plaintiff for intentional or willful refusal by parties subject to this Agreement to comply with the Act.

i. Civil Remedies.

(1) In any suit brought under the provisions of 5 U.S.C. § 552a(g)(1)(C) or (D) in which the court determines that the parties subject to this Agreement acted in a manner

which was intentional or willful, shall be liable in an amount equal to the sum of —

(a) actual damages sustained by the individual because of the refusal or failure, but in no case, shall a person entitled to recovery receive less than the sum of $1,000; and

(b) the costs of the action together with reasonable attorney fees as determined by the court.

(2) An action to enforce any liability created under 5 U.S.C. § 552a may be brought in the district court of the United States in the district in which the complainant resides, or has his principal place of business, or in which the records are situated, or in the District of Columbia, without regard to the amount in controversy, within two years from the date on which the cause of action arises, except that where parties subject to this Agreement have materially and willfully misrepresented any information required under this section to be disclosed to an individual and the information so misrepresented is material to establishment of the liability of the agency to the individual under 5 U.S.C. § 552a, the action may be brought at any time within two years after discovery by the individual of the misrepresentation. Nothing in this section shall be construed to authorize any civil action because of any injury sustained as the result of a disclosure of a record prior to September 27, 1975.

ii. Criminal Penalties

(1) Any officer or employee of an agency, who by virtue of his employment or official position, has possession of, or access to, agency records which contain individually identifiable information the disclosure of which is prohibited by this section or by rules or regulations established thereunder, and who knowing that disclosure of the specific material is so prohibited, willfully discloses the material in any manner to any person or agency not entitled to receive it, shall be guilty of a misdemeanor and fined not more than $5,000. See 5 U.S.C. § 552a(i)(1).

(2) Any officer or employee of any agency who willfully maintains a system of records without meeting the notice requirements of subsection (e)(4) of this section shall be guilty of a misdemeanor and fined not more than $5,000. See 5 U.S.C. § 552a(i)(2).

(3) Any person who knowingly and willfully requests or obtains any record concerning an individual from an agency under false pretenses shall be guilty of a misdemeanor and fined not more than $5,000. See 5 U.S.C. § 552a(i)(3).

6. Child Support FPLS Requirements (If applicable)

a. Contractor and the applicable State of Oklahoma agency must comply with the security requirements established by the Social Security Act, the Privacy Act of 1974, the Federal Information Security Management Act of 2002 (FISMA), 42 United States Code (USC) 654(26), 42 UCS 654a(d)(1)-(5), the U.S. Department of Health and Human Services (HHS), the U.S. Department of Health and Human Services Administration of

Children and Families Office of Child Support Enforcement Security Agreement and the Automated Systems for Child Support Enforcement: A Guide for States Section H Security and Privacy. Contractor and applicable State of Oklahoma agency also agree to use Federal Parent Locator Service (FPLS) information and Child Support (CS) program information solely for the authorized purposes in accordance with the terms in this agreement. The information exchanged between state Child Support agencies and all other state program information must be used for authorized purposes and protected against unauthorized access to reduce fraudulent activities and protect the privacy rights of individuals against unauthorized disclosure of confidential information.

i. This is applicable to the personnel, facilities, documentation, data, electronic and physical records and other machine-readable information systems of the applicable State of Oklahoma agency and Contractor, including, but not limited to, state employees and contractors working with FPLS information and CS program information and state CS agency data centers, statewide centralized data centers, contractor data centers, state Health and Human Services' data centers, comprehensive tribal agencies, data centers serving comprehensive tribes, and any other individual or entity collecting, storing, transmitting or processing FPLS information and CS program information. This is applicable to all FPLS information, which consists of the National Directory of New Hires (NDNH), Debtor File, and the Federal Case Registry (FCR). The NDNH, Debtor File and FCR are components of an automated national information system.

ii. This is also applicable to all CS program information, which includes the state CS program information, other state and tribal program information, and confidential information. Confidential information means any information relating to a specified individual or an individual who can be identified by reference to one or more factors specific to him or her, including but not limited to the individual's Social Security number, residential and mailing addresses, employment information, and financial information. Ref. 45 Code of Federal Regulations (CFR) 303.21(a).

7. FERPA Requirements (If applicable)

a. In performance of this Agreement, Contractor agrees to comply with and assume responsibility for compliance by its employees with the Family Educational Rights and Privacy Act; (20 U.S.C. § 1232g; 34 CFR Part 99) ("FERPA") and the Oklahoma Student Data Accessibility, Transparency, and Accountability Act of 2013; (70 O.S. § 3-168), where personally identifiable student education data is exchanged.

8. CJIS Requirements (If applicable)

a. INTRODUCTION

The use and maintenance of all items of software or equipment offered for purchase herein must be in compliance with the most current version of the U.S. Department of Justice, Federal Bureau of Investigation ("FBI"), Criminal Justice Information Services (CJIS) Division's CJIS Security Policy ("CJIS Security Policy" or "Security Policy" herein).

The Entity or Affiliate acquiring the data or system is hereby ultimately responsible for compliance with the CJIS Security Policy and will be subject to an audit by the State of Oklahoma CJIS Systems Officer ("CSO") and the FBI CJIS Division's Audit Staff.

b. CJIS SECURITY POLICY REQUIREMENTS GENERALLY

The CJIS Security Policy outlines a number of administrative, procedural, and technical controls agencies must have in place to protect Criminal Justice Information ("CJI"). Our experience is that agencies will generally have many of the administrative and procedural controls in place but will need to implement additional technical safeguards in order to be in complete compliance with the mandate. A Criminal Justice Agency ("CJA") and certain other governmental agencies procuring technology equipment and services that could be used in hosting or connecting or transmitting or receiving CJI data may need to use the check list herein to make sure that the software, equipment, location, security, and persons having the ability to access CJI will meet the CJIS requirements per the then current CJIS Security Policy. A completed Appendix H to said Security Policy will need to be signed by Vendor or a 3rd party if it has access to CJI, such as incident to the maintenance or support of the purchased hardware or software within which resides CJI. Per Appendix "A" to said Security Policy, "access to CJI is the physical or logical (electronic) ability, right or privilege to view, modify or make use of CJI."

c. DIRECTIVE CONCERNING ACCESS TO CRIMINAL JUSTICE INFORMATION AND TO HARDWARE OR SOFTWARE WHICH INTERACTS WITH CJI AND CERTIFICATION

The FBI CJIS Division provides state-of-the-art identification and information services to the local, state, tribal, federal, and international criminal justice communities for criminal justice purposes, as well as the noncriminal justice communities for noncriminal justice purposes.

This Directive primarily concerns access to CJI and access to hardware and software in the use, retention, transmission, reception, and hosting of CJI for criminal justice purposes and not for noncriminal justice purposes. In that regard, this Directive is not only applicable to such data, but also to the hardware and software interacting with such data, their location(s), and persons having the ability to access such data. The CJIS data applicable to the Security Policy is the data described as such in said Policy plus all data transmitted over the Oklahoma Law Enforcement Telecommunications System ("OLETS") which is operated by DPS.

In order to have access to CJI or to the aforesaid hardware or software, the vendor must be familiar with the FBI CJIS Security Policy, including but not limited to the following portions of said Security Policy:

1. the Definitions and Acronyms in §3 & Appendices “A” & “B”;
2. the general policies in §4;
3. the Policies in §5;
4. the appropriate forms in Appendices “D”, “E”, “F” & “H”; and
5. the Supplemental Guidance in Appendices “J” & “K”.

This FBI Security Policy is located and may be downloaded at: https://www.fbi.gov/services/cjis/cjissecurity-policy-resource-center.

By executing the Contract to which this Directive is attached, the vendor hereby CERTIFIES that the foregoing directive has and will be followed, including but not limited to full compliance with the FBI CJIS Security Policy, as amended and as applicable.

Attachment B

Public Sector EULA

Commercial Supplier Agreement Header:
This Commercial Supplier Agreement and SAAS License Agreement and Services ("Agreement") is between the Customer, identified in the Purchase Order, Annex, Statement of Work, or similar document, having its principal place of business as set forth in said document, and t UiPath Inc. ("Company" or "Supplier") with its principal place of business at 90 Park Ave, New York, NY, 10016, USA. This Agreement governs the Customer's use of the Supplier software (the "Licensed Software") and the Supplier documentation made available for use with such software. "You" or "Customer" or "Licensee" means the Government Customer (Agency) who is the "Ordering Activity" which is defined as "an entity authorized to order" as may be amended from time to time.

1. DEFINITIONS

"UiPath" means (a) when Customer is located in in North America (meaning United States and its territories, Canada or Mexico): UiPath Incorporated, located in New York, New York, United States; (b) when Customer is located outside North America: UiPath SRL, located in Bucharest, Romania;

"UiPath Partner" means an entity with which UiPath has a valid Partner contract in place for promoting or reselling UiPath RPA Platform or for placing and processing orders from end users;

"Agreement" means these terms and any other terms referenced in this document;

"Affiliate" means any entity that directly or indirectly Controls, is Controlled by, or is under common Control with a party where Control means control of greater than 50 % of the voting rights or equity interests of a party;

„Authorized Users" means either party's employees, representatives and contractors;

"

"Claim" means a claim, action, or legal proceeding filed against a Party;

"Customer" means the Ordering Activity identified in the Order as "Customer" or "Ordering Customer" or otherwise identified in the Order as the end user customer; For the avoidance of doubt, if a Customer Affiliate places an Order under this Agreement, such Affiliate shall be deemed as "Customer" for the purpose of that Order;

"Customer Data" means any information that is imported by or on behalf of Customer into the UiPath RPA Platform from its internal data stores or other sources not supplied by UiPath;

"Development Outputs" means any programs, artifacts, charts or workflow diagrams created by the Customer using UiPath RPA Platform, including any Customer Data;

"Improvements" means all versions, updates, corrections, improvements, developments, modifications, enhancements, variations, derivative works, scripts, customizations, adaptations or extensions of feature sets of any of the UiPath RPA Platform components, created or acquired by UiPath;

"Intellectual Property Rights" means patents, rights to inventions, copyright and related rights, trademarks, trade names and domain names, rights in computer software, and any other intellectual property rights or rights of a similar nature.

"UiPath RPA Platform" means the suite of software components (including Manuals or other documentation) with all Improvements;

"License Term" means the duration of the license for UiPath RPA Platform (or for the provision of Professional Services), as specified in the Order, or any shorter term occurring due to the termination of the Agreement;

"License Key" means an electronic activation key that authorizes the use of the UiPath RPA Platform components;

"Manuals" means the official Product guides available on UiPath website or successor website (except for any marketing, promotional or publicity materials);

"Order" means the order form or other written document for the UiPath RPA Platform, support or Professional services that is either (a) executed between UiPath and an Ordering Activity or (b) the document executed between an UiPath Partner and Customer; If Customer is located in North America the Order will be placed with UiPath Inc., while Customer located in the rest of the world is required to place a PO with UiPath SRL;

"PII" means any information related to an identified or identifiable natural person, including any sensitive data, as defined by Regulation (EU) 2016/679 (GDPR) and other applicable privacy laws and PHI means information about health status, provision or payment of healthcare, which can be linked to an individual (as defined by the Health Insurance Portability and Accountability Act of 1996 (HIPAA).

"Products" means software, with any and all additional versions, updates, enhancements, developments, modifications, derivative works, scripts, connectors, plugins, SDKs, APIs, or extensions thereof, and the underlying Manuals, including any hosted service provided by UiPath, subject to the available licensing models **(Licensing Models).**

"Professional Services" or "PS" means any consulting, training, implementation, or technical services provided by UiPath to a Customer specified in an Order, excluding support services.

1. **Governance.** This Agreement applies to UiPath's Products and PS. Customer's use of new features or functionality of Products not contemplated as of the Effective Date which may be subject to additional terms made available within such Products, shall be deemed acceptance of such additional terms.

2. LICENSES

2.1 License. UiPath grants to the Customer a limited, non-exclusive right to use the components of the UiPath RPA Platform specified in the Order during the License Term, including for testing and disaster recovery purposes. Customer retains all rights, including Intellectual Property Rights, in the Development Outputs created by the Customer with the UiPath RPA Platform, in accordance with this Agreement.

2.2 Trial License. A trial license is subject to the terms located at the following web address and a current copy of which is attached hereto: https://www.uipath.com/hubfs/download/legalspot/21-06-17-Trial-General-Terms.pdf (or successor website). For Trial Licenses, Terms and Conditions are subject to change with the addition of new trial services or removal of existing trial services.

3. THIRD-PARTY ACCESS

3.1 Use by Affiliate and Outsourcing. Customer may allow its Affiliates, including a third-party contractor to operate or access the UiPath RPA Platform solely on Customer's or its Affiliates behalf, but only if it is for Customer's or it's Affiliates direct beneficial business purposes. At UiPath's request, Customer or its Affiliates will specify which entities have access under this provision.

3.2 Customer Responsibility. If Customer allows any person or entity to operate, use or access the UiPath RPA Platform, Customer is responsible for ensuring that such person or entity complies with the terms of this Agreement.

3.3 No Additional Rights. For clarity, the rights granted under this section do not modify the license permissions or increase the number of licenses granted under this Agreement.

4. SUPPORT SERVICES. Support services provided for UiPath RPA Platform are included in the License Fee, in accordance with the Support Terms attached. UiPath may from time to time update the terms provided there is no degradation in the level of service provided. A copy of the current terms are attached and available at: https://www.uipath.com/hubfs/legalspot/UiPath_Support_Terms.pdf

5.RESERVED

6. THIRD PARTY INTELLECTUAL PROPERTY CLAIMS

6.1. UiPath Obligations. UiPath will defend to the extent permitted by 28 U.S.C. 516, at its expense, any third-party Claim against Customer during the License Term to the extent the Claim alleges that the UiPath RPA Platform infringes the third party's patent, copyright, or trademark; or that UiPath has misappropriated the third party's trade secret ("IP Claim"). UiPath will pay any damages finally awarded by a court of competent jurisdiction (or settlement amounts agreed to in writing by UiPath).

6.2 Remedy. In case of any IP Claim, UiPath may: (a) procure for Customer a license to continue using UiPath RPA Platform under the terms of this Agreement; or (b) replace or modify the allegedly infringing components so that they become non-infringing (including disabling the challenged functionality), provided the modified Products remain substantially equivalent in function to the enjoined Products and repurchase the affected components, if any, for which no non-infringing modification is possible in UiPath's determination at a negotiated and mutually-agreeable price that reflects the pro-rata prepaid fees paid by Customer as of the date of UiPath's notification to Customer that no non-infringing modification is possible, but only if Customer confirms in writing that it destroyed all copies of the UiPath RPA Platform component (and any related materials) from all computer systems on which it was stored.

6.3 Conditions. UiPath will have no liability for any IP Claim: (A) that arises from any: (i) use of the UiPath RPA Platform in violation of this Agreement; (ii) modification of the UiPath RPA Platform by anyone other than UiPath; (iii) failure by Customer to install the latest updated version of the UiPath RPA Platform, as requested by UiPath to avoid infringement; or (iv) third-party products, services, hardware, software, or other materials, or combination of these with the UiPath RPA Platform, if the UiPath RPA Platform would not be infringing without this combination; or (B) if Customer fails to: (i) promptly notify UiPath in writing of the IP Claim; (ii) provide UiPath with reasonable assistance requested by UiPath for the defense of the IP Claim; (iii) provide UiPath with the exclusive right to control or settle the IP Claim; or (iv) refrain from making admissions about the IP Claim without UiPath's prior written consent. Notwithstanding the foregoing, the United States Department of Justice reserves the right to take sole control over the defense and settlement of Third-Party Claims. The remedies in this section are Customer's sole and exclusive remedies and UiPath's sole liability regarding the subject matter giving rise to any IP Claim.

7. OTHER CLAIMS

7.1. Customer's Obligations. Intentionally omitted.

7.2 Conditions. Customer's obligations under this section are conditioned upon UiPath (to the extent permitted by applicable law): (i) promptly notifying the Customer of any Claim in writing; (ii) cooperating with the Customer in the defense of the Claim; (iii) granting the Customer control of the defense or settlement of the Claim to the extent permitted by 28 U.S.C. 516; and (iv) refraining from making any admissions about the Claim. The remedies in this section are UiPath's sole and exclusive remedies and Customer's sole liability regarding the subject matter giving rise to any such Claim.

8. LIMITATION OF LIABILITY

8.1. Damages Exclusion. Neither Party will be liable to the other Party for any special, indirect, moral, consequential, incidental, punitive, or exemplary damages; the use or inability to use the UiPath RPA Platform, computer malfunction or failure, server down time, failure of the UiPath RPA Platform to operate with any other programs, loss of profits; loss of reputation, use, or revenue; loss or corruption of data; or interruption of business. Under no circumstances may UiPath or its Affiliates be liable for any claims that may be asserted, granted or imposed against, arising from, or in connection with, Customer Data except as otherwise set forth herein.

8.2 Liability Cap. The maximum aggregate liability of each Party for each and all Claims (individually and together) under or relating to this Agreement or its subject matter will not exceed the total subscription license fees paid under this Agreement during the 12 months before the initial Claim. This limitation will apply whether an action is in contract or tort and regardless of the theory of liability. This clause shall not impair the U.S. Government's right to recover for fraud or crimes arising out of or related to this Government Contract under any federal fraud statute, including the False Claims Act, 31 U.S.C. §§ 3729-3733.

8.3 Other Responsibility. For the avoidance of any doubt, under no circumstances UiPath may be liable for any Claims, judgments, awards, costs, expenses, damages and liabilities (including reasonable attorneys' fees) of any kind and nature that may be asserted, granted or imposed against, directly or indirectly, arising from or in connection to any Customer Development Outputs. This clause shall not impair the U.S. Government's right to recover for fraud or crimes arising out of or related to this Government Contract under any federal fraud statute, including the False Claims Act, 31 U.S.C. §§ 3729-3733.

9. REPRESENTATIONS & WARRANTIES

9.1 UiPath RPA Platform Limited Warranty and Remedy. UiPath warrants that the UiPath RPA Platform, as delivered to Customer, will substantially conform to the applicable Manuals during the License Term, to the extent that the UiPath RPA Platform is used in accordance with the Manuals. Customer must notify UiPath of a Claim under this warranty within 30 days of the date on which the condition giving rise to the Claim first appeared. To the extent permitted by law, Customer's sole and exclusive remedy and UiPath's sole liability under or about this warranty will be a replacement of the UiPath RPA Platform component, or if replacement is not commercially reasonable, a suspension of the applicable UiPath RPA Platform component or services and a refund of any pre-paid unused fees for the applicable UiPath RPA Platform component or service.

9.2 Implied Warranties. Except for the express warranties herein, UiPath RPA Platform is provided on an "as-is" basis. Neither party makes any warranty of any kind, whether express, implied, statutory or otherwise, and each party specifically disclaims all implied warranties, including any implied warranties of merchantability, fitness for a particular purpose or non-infringement, to the maximum extent permitted by applicable law. Customer bears the entire risk as to the use of the UiPath RPA Platform. Each party disclaims all liability for any harm or damages caused by any third-party hosting providers. In the event of a breach of warranty, the U.S. Government reserves all rights and remedies under the contract, the Federal Acquisition Regulations, and the Contract Disputes Act, 41 U.S.C. 7101-7109.

10. TERM

10.1 Duration. This Agreement applies to the UiPath RPA Platform from the Effective Date until the expiration of the applicable License Term or the term for Professional Services as set forth in an Order or applicable statement of work.

10.2 Material Breach. If either Party commits a material breach of this Agreement, the non-breaching Party may give written notice describing the nature and basis of the breach to the breaching Party.

10.3 Effect of Termination. Upon termination or expiration of this Agreement or any License Term the license and associated rights for the UiPath RPA Platform will immediately terminate and Customer must, at its expense remove and delete all copies of the UiPath RPA Platform. Some or all the UiPath RPA Platform components may cease to operate without prior notice upon expiration or termination of the License Term.

11. PROFESSIONAL SERVICES

11.1 License to Deliverables. If it is the case, UiPath grants Customer a non-exclusive, non-sublicensable and non-transferable license to use the materials developed and provided to Customer by UiPath in performing the Professional Services ("Deliverables") solely for Customer's beneficial business purposes.

11.2 Employment Taxes. UiPath is responsible for all taxes and any employment obligations arising from its employment of personnel and contractors used to perform the Professional Services.

11.3 Warranty. UiPath warrants the Professional Services will be performed in a professional and workmanlike manner. Customer must notify UiPath in writing of any breach of this warranty within 30 days of delivery of such Professional Service. To the extent permitted by law, Customer's sole and exclusive remedy for breach of this warranty will be re-performance of the relevant Professional Service.

11.4 Subcontractors. Customer agrees that UiPath may use subcontractors for which UiPath will be responsible, in the performance of the Professional Services.

11.5 No Personal Data. During the performance of Professional Services, Customer needs to avoid transmission to UiPath of information that is regulated by applicable privacy laws ("Personal Data") (for example, by using "dummy data" when configuring or testing solutions). UiPath does not wish to receive Personal Data nor is it required for the performance of the Professional Services. Accordingly, Customer must not transmit Personal Data to UiPath, unless the Parties have agreed in writing on terms specifying that UiPath has agreed to receive Personal Data and detailing the security measures in place and protocol for the processing of Personal Data.

12. **Data**

12.1 **Data Collection**. Each Party may collect, store and use PII of the other Party's personnel necessary for the Agreement by complying with the applicable privacy laws. UiPath or its Affiliates may also collect and analyze diagnostic, technical, error reports, crash dumps, usage and other telemetry data from Customer's use of the Products and Customer grants them a worldwide, transferable, royalty-free right to access, use and process such data for the purpose of providing and updating the Products or PS, offering support and addressing technical issues, and as required by law or as reasonably provided in the Privacy Policy available on UiPath's website (or

successor). Customer will inform its own personnel for the processing of their PII in accordance with the applicable laws. UiPath processes PII as described in its Privacy Policy available on its website.

11.7 **Use of Data**. Use of Products or PS does not require PII and UiPath accepts no liability thereof. However, if Customer uses Products lawfully on UiPath servers/cloud, PII may be transferred to UiPath, who will be considered a processor on behalf of the Customer and the data processing agreement available on UiPath's website will apply from the moment of the transfer. Customer must not use PHI on UiPath servers/cloud. If provision of PS is rendered impossible due to the lack of PII, Customer will notify UiPath and the Parties will discuss entering into a data processing agreement.

12. GENERAL

12.1 . Intentionally omitted.

12.2 Customer's Purchase Order. Any terms or conditions in Customer's purchase order or any other related documentation submitted by or on behalf of Customer to UiPath (or any other party, such as an UiPath Partner) do not form part of this Agreement and are void, unless otherwise expressly agreed in writing and signed by both Customer and UiPath.

12.3 Confidentiality Obligations. Parties must keep the Confidential Information (means and refers to any document and information to which a Party has access during the performance of this Agreement, including but not limited to technical information, business methods, software programs, licensing model, of the other Party) confidential. Neither Party will in any manner, directly or indirectly, use or otherwise employ all or any of the Confidential Information of the other Party for any purpose other than the performance under this Agreement. This confidentiality obligation will survive for 3 years after the termination or expiration of this Agreement. The Customer acknowledges that if it provides any suggestions or feedback to UiPath, it does so voluntarily and without any obligation of confidence on UiPath in relation thereto who will be entitled to use any suggestions or feedback, in any way and for any purpose.

12.4 Data Use Consent. Customer agrees that UiPath and its Affiliates may collect and use technical information gathered as part of the software support services provided, if any, related to the UiPath RPA Platform. UiPath may use this information solely to improve the software or to provide customized services or technologies to the Customer and will not disclose this information in a form that personally identifies the Customer.

12.5 Entire Agreement. This agreement and any orders issued thereunder constitute the entire agreement. Any amendments to this Agreement may only be made in writing and become effective when signed by both Parties.

12.6 Governing Law, Venue. The validity, interpretation and enforcement of this Agreement will be governed by and construed in accordance with the laws of the United States. In the event the Uniform Computer Information Transactions Act (UCITA) or any similar federal laws or regulations are enacted, to the extent allowed by law, it will not apply to this Agreement, and the governing law will remain as if such law or regulation had not been enacted. Any disputes relating to this Agreement shall be resolved in accordance with the FAR, and the Contract Disputes Act, 41 U.S.C. §§ 7101-7109.

12.7 License Compliance. UiPath may, at its expense and no more than once every 12 months, appoint its own personnel or an independent third party (or both) to verify that Customer's use, installation, or deployment of the UiPath RPA Platform comply with the terms of this Agreement and Customer agrees to provide all the required assistance and support during such verification. This inspection will be subject to any security requirements.

12.8 No Partnership. Nothing in this Agreement is intended to constitute a fiduciary relationship, agency, joint venture, partnership, or trust between the Parties and neither Party has authority to bind the other Party.

12.9 Notices. Any notice given under this Agreement must be in writing by email to the following addresses (or addresses notified in writing by either Party): to UiPath: legal@uipath.com; and to Customer: at Customer's email address stated on the Order, or if Customer's Order is with an UiPath Partner, at Customer's registered address and will be effective when received by the Party, or refused by the Party.

12.10 Publicity.. Any publicity related to the Government's use of this service must be pre-approved in writing by the Government Contracting Officer.

12.11 Privacy. If UiPath receives Personal Data of the Customer personnel involved in the performance of this Agreement it will process it in accordance with the UiPath Privacy Policy available on its website.

12.12 Severability. If any provision of this Agreement is or becomes illegal, invalid or unenforceable for any reason, all other provisions of the Agreement remain in force and shall produce legal effects.

12.13 Third Party Providers. If Customer uses certain features of the UiPath RPA Platform in conjunction with third party data, products, services, and platforms, then Customer is responsible for complying with the terms and conditions required by such third-party providers, and all such use is at Customer's own risk.

12.14 Third Party Licenses. The UiPath RPA Platform contains components of other software, including open source, which are the property of their respective owners and are licensed under their respective licenses specified on Third Party Licenses section on UiPath website, as updated from time to time or communicated to the Customer.

12.15 Export. UiPath RPA Platform may be subject to the trade control laws and regulations of the United States and other national governments. Each party represents that it is not named on any E.U. or U.S. government denied-party list and will not use UiPath RPA Platform in a E.U. or U.S. embargoed country (currently Cuba, Iran, North Korea, Sudan, Syria or Crimea) or in violation of any E.U. or U.S. export law or regulation.

12.16 Anti-Corruption. Each party confirms it has not been offered or received any illegal or improper bribe, kickback, payment, gift, or thing of value from the other party's employees or agents in connection with this Agreement. Reasonable gifts and entertainment provided in the ordinary course of business do not violate the above restriction. Any violation of the above restriction, will be promptly notified to legal@uipath.com

12.17 Waiver. No failure to exercise, nor any delay in exercising, any right, power or remedy under this Agreement shall operate as a waiver, nor shall any single or partial exercise of any right or remedy prevent any further or other exercise or the exercise of any other right or remedy. The rights and remedies provided in this Agreement are cumulative and not exclusive of any rights or remedies (provided by law). Any waiver of any breach of this Agreement.