**ENTERPRISE SAAS SOFTWARE/SERVICES LICENSE
REQUIREMENTS AGREEMENT
BETWEEN
THE COMMONWEALTH OF PENNSYLVANIA,
ACTING BY AND THROUGH THE GOVERNOR'S OFFICE OF ADMINISTRATION
AND**

_____

This Enterprise SaaS Software/Services License Requirements Agreement ("Agreement") is entered into by and between _____ ("Licensor") and the **Commonwealth of Pennsylvania**, acting by and through the **Governor's Office of Administration** ("Commonwealth").

The parties intending to be legally bound, agree as follows:

1.   **Order of Precedence**. The terms and conditions of this Agreement, to the extent a conflict exists, supersede and take precedence over the terms and conditions of the Licensor [insert the name of Licensor's standard End User License/Software License Agreement], which is attached to this Agreement as Exhibit A. The terms of this Agreement supersede and take precedence over the terms included in any quote, purchase order, terms of any shrink-wrap agreement included with the Licensed Products, terms of any click through agreement included with the Licensed Products or any other terms purported to apply to the Licensed Products. The products specified in Attachment 1, along with maintenance, support and services for said products, shall be referred to as "Licensed Products."

2.   **Effective Date**. The effective date of this Agreement shall be the date that it has been fully executed by the Licensor and by the Commonwealth and all approvals required by Commonwealth contracting procedures have been obtained.

3.   **Enterprise Language**.

     (a)   The parties agree that more than one agency of the Commonwealth ("Commonwealth Agency") may license products subject to this Agreement, provided that the procurement of any Licensed Products by any Commonwealth Agency must be made pursuant to one or more executed purchase orders or purchase documents submitted by each Commonwealth Agency seeking to use the Licensed Products.

     (b)   The parties agree that, if the licensee is a "Commonwealth Agency" as defined by Section 103 of the *Commonwealth Procurement Code*, 62 Pa. C. S. § 103, the terms and conditions of this Agreement apply to the procurement of any Licensed Products made by the Commonwealth, and that the terms and conditions of this

Agreement become part of the purchase order or other procurement document without further need for execution.

4.   List of Licensed Products.

(a)   Attached hereto and made a part of this Agreement by reference is Attachment 1, which lists the Licensed Products that may be licensed under this Agreement. With the consent of the Commonwealth, the list of Licensed Products on Attachment 1 may be updated by the Licensor providing the Commonwealth with a revised Attachment 1 that adds the new product to the list. The Commonwealth, in its sole discretion, may consent either via written communication directly to the Licensor or, if applicable, providing the Commonwealth's reseller with a copy of Licensor's notification to update Attachment 1.

(b)   No amendment will be required to add a new Licensed Product to the list. If, however, the Licensor desires to add a new Licensed Product to the list that requires additional licensing terms or other requirements, either an amendment to this Agreement or a new agreement will be required.

5.   Choice of Law/Venue. This Agreement shall be interpreted in accordance with and governed by the laws of the Commonwealth of Pennsylvania, without giving effect to its conflicts of law provisions. The courts of the Commonwealth of Pennsylvania and the federal courts of the Middle District of Pennsylvania shall have exclusive jurisdiction over disputes under this Agreement and the resolution of those disputes.

6.   Indemnification.

(a)   The Licensor shall indemnify the Commonwealth against all third-party claims, suits, demands, losses, damages, costs, and expenses, including without limitation, litigation expenses, attorneys' fees, and liabilities, arising out of or in connection with any activities performed by the Licensor or its employees and agents that are related to this Agreement, as determined by the Commonwealth in its sole discretion.

(b)   The Commonwealth shall provide the Licensor with prompt notice of any claim or suit of which it learns. Pursuant to the Commonwealth Attorneys Act (71 P.S. Section 732-101, et seq.), the Office of Attorney General (OAG) has the sole authority to represent the Commonwealth in actions brought against the Commonwealth. The OAG may, however, in its sole discretion and under any terms as it deems appropriate, delegate its right of defense. If OAG delegates the defense to the Licensor, the Commonwealth will cooperate with all reasonable requests of Licensor made in the defense of such suits.

(c)   Notwithstanding the above, neither party may enter into a settlement of any claim or suit without the other party's written consent, which will not be unreasonably

withheld. The Commonwealth may, in its sole discretion, allow the Licensor to control the defense and any related settlement negotiations.

7.   Sovereign Immunity.

No provisions of this Agreement may be construed to waive or limit the sovereign immunity of the Commonwealth of Pennsylvania or its governmental sub-units.

8.   Patent, Copyright, Trademark and Trade Secret Protection.

(a)   The Licensor shall, at its expense, defend, indemnify and hold the Commonwealth harmless from any suit or proceeding which may be brought by a third party against the Commonwealth, its departments, officers or employees for the alleged infringement of any United States patents, copyrights, trademarks or trade dress, or for a misappropriation of a United States trade secret arising out of performance of this Agreement ("Claim"), including all Licensed Products provided by the Licensor. For the purposes of this Agreement, "indemnify and hold harmless" shall mean the Licensor's obligation to (a) pay any judgments, fines and penalties finally awarded by a court of competent jurisdiction, governmental/administrative body or any settlements reached pursuant to a Claim and (b) reimburse the Commonwealth for its reasonable administrative costs or expenses, including without limitation reasonable attorney's fees, it necessarily incurs in handling the Claim. The Commonwealth shall give the Licensor prompt notice of any such claim of which it learns. Pursuant to the *Commonwealth Attorneys Act,* Act of October 15, 1980, P.L. 950, No. 164, as amended, 71 P. S. §§ 732-101—732-506, the Office of Attorney General ("OAG") has the sole authority to represent the Commonwealth in actions brought against the Commonwealth. The OAG, however, in its sole discretion, and under the terms the OAG deems appropriate, may delegate its right of defense of a Claim. If the OAG delegates the defense to the Licensor, the Commonwealth will cooperate with all reasonable requests of the Licensor made in the defense of and/or settlement of a Claim. The Licensor shall not, without the Commonwealth's consent, enter into any settlement agreement which (a) states or implies that the Commonwealth has engaged in any wrongful or improper activity other than the innocent use of the material which is the subject of the Claim, (b) requires the Commonwealth to perform or cease to perform any act or relinquish any right, other than to cease use of the material which is the subject of the Claim, or (c) requires the Commonwealth to make a payment which the Licensor is not obligated by this Agreement to pay on behalf of the Commonwealth. In all events, the Commonwealth shall have the right to participate in the defense of any such suit or proceeding through counsel of its own choosing. It is expressly agreed by the Licensor that, in the event it requests that the Commonwealth provide support to the Licensor in defending any such Claim, the Licensor shall reimburse the Commonwealth for all necessary expenses (including attorneys' fees, if such are made necessary by the Licensor's request) incurred by the Commonwealth for such support. The Licensor, at its own expense, shall provide whatever cooperation the OAG requests in the defense of the Claim.

(b)   The Licensor shall exercise reasonable due diligence to prevent claims of infringement on the rights of third parties. The Licensor certifies that, in all respects applicable to this Agreement, it has exercised and will continue to exercise due diligence to ensure that all Licensed Products provided under this Agreement do not infringe on the patents, copyrights, trademarks, trade dress, trade secrets or other proprietary interests of any kind which may be held by third parties.

(c)   If the defense of a Claim and the authority to control any potential settlements of a Claim is delegated to the Licensor, the Licensor shall pay all damages and costs finally awarded against the Commonwealth or agreed to by the Licensor in any settlement. If information and assistance are furnished by the Commonwealth at the Licensor's written request, it shall be at the Licensor's sole expense.

(d)   If any Licensed Product furnished hereunder is likely to (in the Licensor's opinion) or does become subject to a claim of infringement of a United States patent, copyright, trade dress or trademark, or for a misappropriation of trade secret, or is held to constitute infringement and the use of the Licensed Product is enjoined, without diminishing the Licensor's obligation to satisfy any final award, the Licensor may, at its option and expense:

   (i)   Replace or substitute functional equivalents for the Licensed Product;

   (ii)   Modify the Licensed Product so that it is no longer infringing;

   (iii)   Re-perform the Services in a non-infringing manner; or

   (iv)   obtain the rights necessary for the Licensor to continue performance under this Agreement or obtain the rights for the Commonwealth to continue the use of the Licensed Product.

(e)   If the use of any Licensed Product is enjoined and the Licensor is unable to provide any remedy set forth in subsection (d) above, the Licensor, upon return of the Licensed Product, shall refund to the Commonwealth:

   (i)   the fee paid for the infringing Licensed Product, less the amount for the period of usage of the Licensed Product; and

   (ii)   the pro-rated portion of any maintenance fees representing the time remaining in any period of services for which payment was made.

(f)   The obligations of the Licensor under this section survive the termination of this Agreement.

(g)   Notwithstanding the above, the Licensor shall have no obligation under this section to the extent a Claim arises from:

(i)   modification of any Licensed Products provided by the Commonwealth or a third party acting under the direction of the Commonwealth;

(ii)   any material provided by the Commonwealth to the Licensor and incorporated into, or used to prepare any Licensed Products;

(iii)   use of any Licensed Product after the Licensor recommends discontinuation because of possible or actual infringement and has provided one of the remedies under subsection (e) or subsection (f) above;

(iv)   use of any Licensed Product in other than the specified operating environment;

(v)   the combination, operation, or use of the Licensed Products with other products, services, or deliverables not provided by the Licensor as a system or the combination, operation, or use of the Licensed Products, service, or deliverable, with any products, data, or apparatus that the Licensor did not provide;

(vi)   infringement of a non-Licensed Product alone;

(vii)   the Commonwealth's use of any Licensed Product beyond the scope contemplated by the Agreement; or

(viii) the Commonwealth's failure to use corrections or enhancements made available to the Commonwealth by the Licensor at no charge.

9.   Virus, Malicious, Mischievous or Destructive Programming.

(a)   The Licensor warrants that the Licensed Products as delivered by the Licensor does not contain any viruses, worms, Trojan Horses, or other malicious or destructive code to allow unauthorized intrusion upon, disabling of, or erasure of the Licensed Products (each a "Virus"). However, the Licensed Products may contain a key limiting use to the scope and quantity of the license(s) granted, and license keys issued by the Licensor for temporary use are time-sensitive.

(b)   The Licensor shall be liable to the Commonwealth for any damages, costs, fines, remedial measures incurred by the Commonwealth and shall indemnify the Commonwealth against any Third Party claims (in accordance with Section 6, Indemnification) if the Licensor or any of its employees, subcontractors or consultants introduces a virus or malicious, mischievous or destructive programming into the Licensed Product or the Commonwealth's or Third Party's software, data, systems or computer networks.

10. **Limitation of Liability**.

    (a)   Except as otherwise provided in this Agreement, the Licensor's liability to the Commonwealth under this Agreement shall be limited to the greater of $500,000 or the total dollar amount of purchase orders issued for Licensed Products and services covered by this Agreement during the twelve (12)-month period prior to the event giving rise to the damage claim. This limitation does not apply to damages:

        (i)   for bodily injury;

        (ii)   for death;

        (iii)   for gross negligence and willful or unlawful misconduct;

        (iv)   to real property or tangible personal property for which the Licensor is legally liable;

        (v)   under Section 8, Patent, Copyright, Trade Secret and Trademark Protection;

        (vi)   resulting from a breach of the security of a system maintained or managed by the Licensor, including the costs for notification, mitigation and credit monitoring services required due to such breach;

        (vii)   resulting from a breach of confidentiality;

        (viii)   for which the Licensor is responsible pursuant to any indemnification obligations it has under this Agreement; or

        (ix)   under Section 9, Virus, Malicious, Mischievous or Destructive Programming.

    (b)   Except with respect to those damages enumerated in subsection 10(a)(i) through (ix) above, the Licensor shall not be liable for consequential, indirect, or incidental damages unless otherwise specified in the Agreement.

11. **Payment**.

The Commonwealth will make purchase and make payment through a reseller contract or another procurement document, which shall control with regard to payment amounts and provisions.

12. **Termination**.

    (a)   The Licensor may not terminate for non-payment an order issued through a reseller contract or another procurement document that controls payment.

(b)   The Commonwealth may terminate this Agreement without cause by giving the Licensor **30 calendar days'** prior written notice ("Notice of Termination") whenever the Commonwealth shall determine that such termination is in the best interest of the Commonwealth ("Termination for Convenience").

13.   **Background Checks**.

(a)   Upon prior written request by the Commonwealth, the Licensor must, at its expense, arrange for a background check for each of its employees, as well as for the employees of its subcontractors, who will have access to Commonwealth Confidential Information or Commonwealth facilities, either through on site or remote access. Background checks shall be conducted via the Request for Criminal Record Check for in-state Licensor employees or via a criminal background check through the appropriate State Agency for the out of state Licensor employees. The background check shall be conducted prior to initial access by the Licensor employee and annually thereafter.

(b)   Before the Commonwealth permits an employee access to the Commonwealth Confidential Information or Commonwealth facilities, the Licensor must provide written confirmation to the office designated by the applicable Commonwealth Agency that the background check has been conducted. If, at any time, it is discovered that an employee has a criminal record that includes a felony or misdemeanor involving terrorist threats, violence, use of a lethal weapon, or breach of trust/fiduciary responsibility; or which raises concerns about building, system, or personal security, or is otherwise job-related, the Licensor shall not assign that employee to any Commonwealth facilities, shall remove any access privileges already given to the employee, and shall not permit that employee remote access to Commonwealth facilities, systems or Confidential Information, unless the Commonwealth Agency consents, in writing, prior to the access being provided. The Commonwealth Agency may withhold its consent at its sole discretion. Failure of the Licensor to comply with the terms of this subsection may result in the default of the Licensor under its Agreement with the Commonwealth.

(c)   The Commonwealth specifically reserves the right to conduct background checks over and above that described herein.

14.   **Confidentiality**.

(a)   <u>Definition</u>. "Confidential Information:"

(i)   For the Commonwealth: Information, whether oral or written or via computer disk or electronic media, to which the Licensor is given access, or which is made available by the Commonwealth, whether directly or through a third party, is defined as "Confidential Information." Confidential Information shall include, without limitation, all technology, know-how,

processes, software, databases, Trade Secrets (as defined by the Pennsylvania Uniform Trade Secret Act found at 12 Pa. Cons. Stats Secs. 5392 et. seq.), proprietary information, product and business requirements, and information about or from the Commonwealth's vendors or employees whether received before or after the Effective Date of this Agreement. Confidential Information shall also include information and documentation that is not permitted to be disclosed to third parties under local, Commonwealth or federal laws and regulations or pursuant to any policy adopted by the Commonwealth or pursuant to the terms of any third-party agreement to which the Commonwealth is a party. Sensitive information, as define in Section 15 below, shall be a subset of Confidential Information of the Commonwealth, and shall be subject to additional protections as set forth in Section 15 below.

(ii)   For the Licensor: All information identified in writing by the Licensor as confidential or proprietary to the Licensor or its subcontractors.

(b)   <u>Confidential Information</u>. All Confidential Information of or relating to the disclosing party shall be held in confidence by the receiving party to the same extent and in at least the same manner as the receiving party protects its own confidential or proprietary information, using no less than commercially reasonable standards or higher or more stringent standards required by law, including those laws governing Sensitive Information, and those standard specified in this Agreement. The receiving party shall not disclose, publish, release, transfer or otherwise make available any Confidential Information of the disclosing party in any form to, or for the use or benefit of, any person or entity without the disclosing party's consent. Subject to the other provisions of this Agreement, receiving party shall be permitted to disclose relevant aspects of the disclosing party's Confidential Information to the receiving party's officers, agents, subcontractors and personnel and to the officers, agents, subcontractors and personnel of the receiving party's corporate affiliates or subsidiaries to the extent that such disclosure is reasonably necessary for the performance of the receiving party's duties and obligations under this Agreement; provided, however, that the receiving party shall take all reasonable measures to ensure that Confidential Information of the disclosing party is not disclosed or duplicated in violation of the provisions of this Agreement by such officers, agents, subcontractors and personnel and that the receiving party shall be responsible for any unauthorized disclosure of the Confidential Information by the receiving party's officers, agents, subcontractors or personnel; and further provided, that if the disclosure is by the Commonwealth to another contractor or sub-contractor, such disclosure is subject to a suitable non-disclosure agreement imposing equally or more stringent requirements for data privacy and security. Except for Sensitive Information (which shall be protected in all circumstances), and except to the extent provided otherwise by any applicable law, the obligations of this subsection (b) shall not apply with respect to information that:

(i)   is developed by the other party without violating the disclosing party's proprietary rights;

(ii)   is or becomes publicly known,

(iii)   is disclosed by the owner of such information to a third party free of any obligation of confidentiality;

(iv)   is already known by the receiving party without an obligation of confidentiality other than pursuant to this Agreement or any confidentiality contract entered into before the Effective Date of the Agreement between the Commonwealth and the Licensor; or

(v)   is rightfully received by the receiving party free of any obligation of confidentiality.

(c)   <u>Obligations</u>. Each party shall:

(i)   notify the other party promptly of any known unauthorized possession, use or knowledge of the other party's Confidential Information by any person or entity;

(ii)   promptly furnish to the other party full details known by such party relating to the unauthorized possession, use or knowledge thereof and shall use reasonable efforts to assist the other party in investigating or preventing the recurrence of any unauthorized possession, use or knowledge of the other party's Confidential Information;

(iii)   use reasonable efforts to cooperate with the other party in any litigation and investigation against third parties deemed necessary by the other party to protect its proprietary rights; and

(iv)   promptly use all reasonable efforts to prevent a recurrence of any such unauthorized possession, use or knowledge of the other party's Confidential Information.

(d)   <u>Cost of compliance; required disclosure</u>. Each party shall bear the cost it incurs as a result of compliance with this section. The obligations in this section shall not restrict any disclosure by either party pursuant to any applicable law or pursuant to the order of any court or other legal process or government agency of competent jurisdiction (provided that the receiving party shall give prompt notice to the non-disclosing party of such disclosure or order in a timeframe to allow the disclosing party to resist the disclosure or order).

(e)   Submitting Confidential Information to the Commonwealth. The Licensor shall use the following process when submitting information to the Commonwealth that it believes to be confidential and/or proprietary information or trade secrets:

   (i)   prepare an un-redacted version of the appropriate document;

   (ii)   prepare a redacted version of the document that redacts the information that is asserted to be confidential or proprietary information or a trade secret;

   (iii)   prepare a signed written statement that states:

      (1)   the attached document contains confidential or proprietary information or trade secrets;

      (2)   the Licensor is submitting the document in both redacted and un-redacted format in accordance with Section 707(b) of the *Right-to-Know Law*, 65 P.S. § 67.707(b); and

      (3)   the Licensor is requesting that the document be considered exempt under Section 708(b)(11) of the *Right-to-Know Law,* 65 P.S. § 67.708(b)(11) from public records requests; and

   (iv)   submit the **two (2)** documents with the signed written statement to the Commonwealth.

(f)   Confidential Information at termination. Upon expiration or termination of this Agreement, or a purchase order or other procurement document for Licensed Products governed by the terms of this Agreement, and at any other time at the written request of a party, the receiving party must promptly return to the disclosing party all of the disclosing party's Confidential Information and Data (and all copies of this information) that is in the receiving party's possession or control, regardless of form.

(g)   Not confidential. Additionally, neither this Agreement nor any pricing information related to this Agreement, nor purchase orders issued pursuant to this Agreement, will be deemed confidential.

15.   Sensitive Information.

(a)   "Sensitive Information" is a subcategory of Confidential Information of the Commonwealth and shall include, regardless of whether marked or identified by the Commonwealth as confidential:

   (i)   Information related to the design or implementation of the Commonwealth's technology and security infrastructure and architecture,

including, but not limited to, Protected Critical Infrastructure Information (PCII) under the Cybersecurity Information Sharing Act (CISA) of 2015;

(ii)   Information identified as Sensitive Security Information, Protected Information or Privileged Information as defined under ITP-SEC19;

(iii)   Passwords, encryption keys, and other cyber security control design information;

(iv)   Consumer and citizen information;

(v)   Employee information;

(vi)   Information that is either nonpublic personal information or personally identifiable information, including, without limitation, names, addresses, telephone numbers, fax numbers, electronic mail addresses, web universal resource locators (URLs), Internet Protocol (IP) addresses, vehicle identifiers, account numbers, birthdates, social security numbers, individual likeness or images, fingerprint or biometric data, genetic information, demographic, information contained in, relating to or deriving from medical or personal health records, criminal justice information and records, information relating to drivers licenses or other identification cards, financial and transactional information, tax information and any other information that is deemed to be nonpublic or protected under federal and state law, regulation, order or standard including, but not limited to, the Criminal History Record Information Act, the Family Education Rights and Privacy Act (FERPA), the Health Insurance Portability and Accountability Act (HIPAA), Confidentiality of HIV-Related Information Act, the Omnibus Reconciliation Act of 1990, Real ID Act of 2005, Tax Reform Act of 1976 the Internal Revenue Code and IRS Publication 1075, the Affordable Care Act, federal and state notification laws, The Driver's Privacy Protection Act of 1994, Title V of the *Gramm-Leach-Bliley Act*, Section 628 of the *Fair Credit Reporting Act*, Section 216 of the Fair and Accurate Credit Transactions Act, the *Children's Online Privacy Protection Act*, and any implementing regulations, guidelines and Commonwealth policies adopted under any of these or other related laws; and

(vii)   Payment Card Industry Information (PCI).

(b)   The Licensor understands that its level of access may allow or require it to view or access Sensitive Information and Confidential Information. The Licensor shall hold all Commonwealth Sensitive Information in the strictest of confidence and shall use all protective measures to protect the Sensitive Information as prescribed by law, regulation and/or Commonwealth policies and standards. In addition, the Licensor shall only permit staff located in the United States to access Sensitive

Information, Confidential Information and Commonwealth systems, data and services.

(c)   Sensitive Information and Confidential Information may be subject to and governed by specific state and federal laws, regulations and policies that must be followed. If applicable, prior to deployment of the Products or Services, the Licensor may be required to sign off on particular instructions, restrictions and limitations as dictated by the Commonwealth, including, but not limited to, as necessary, HIPAA Business Associate Agreements. The Commonwealth's use of any sign off sheet shall create specificity in the Licensor's obligations with respect to certain Confidential Information, and this Section and the instructions within the sign-off sheet shall not, in any way, diminish the obligations of the Licensor under this Agreement with respect to Confidential Information generally and Sensitive Information specifically. The sign-off sheet shall be signed by at least one authorized signatory for the Licensor and incorporated into this Agreement.

16.   **Data Breach or Loss**.

(a)   Compliance with Laws. The Licensor shall comply with all applicable data protection, data security, data privacy and data breach notification laws, including, but not limited to, the *Breach of Personal Information Notification Act,* as amended November 2, 2022, P.L. 2139, No. 151, 73 P.S. §§ 2301—2330. Further, to the extent the Licensor maintains, stores, or manages computerized data on behalf of the Commonwealth that constitutes personal information, as defined in the *Breach of Personal Information Notification Act,* the Contractor shall comply with the then current version of the following IT Policies (ITPs): *ITP-SEC019, Policy and Procedures for Protecting Commonwealth Electronic Data*; *ITP-SEC024, IT Security Incident Reporting Policy*; *ITP-SEC025, Proper Use and Disclosure of Personally Identifiable Information (PII)*; and *ITP-SEC031, Encryption Standards*.

(b)   Control of Licensor. For Data and Confidential Information in the possession, custody, and control of the Licensor or its employees, agents, and/or subcontractors:

(i)   The Licensor shall report unauthorized access, acquisition, use, release, loss, destruction or disclosure of Data or Confidential Information ("Incident") to the Commonwealth within one (1) hour of when the Licensor knows of or reasonably suspects such Incident, and the Licensor must immediately take all reasonable steps to mitigate any potential harm or further access, acquisition, use, release, loss, destruction or disclosure of such Data or Confidential Information.

(ii)   The Licensor shall provide timely notice to all individuals that may require notice under any applicable law or regulation as a result of an Incident. The notice must be pre-approved by the Commonwealth. At the Commonwealth's request, the Licensor shall, at its sole expense, provide

credit monitoring services to all individuals that may be impacted by any Incident requiring notice.

    (iii)   The Licensor shall be solely responsible for any costs, losses, fines, or damages incurred by the Commonwealth due to Incidents, which shall be reimbursed upon invoice received from the Commonwealth.

    (iv)   The Licensor shall indemnify the Commonwealth against any third party claims arising out of an Incident.

(c)   <u>Security Breach</u>. Licensor agrees that it shall not inform any third party of any Security Breach without first obtaining the Commonwealth's prior, written consent, other than to inform a complainant that the matter has been forwarded to the Commonwealth's legal counsel. Further, the Licensor agrees that the Commonwealth shall have the sole right to determine: (i) whether notice of the Security Breach is to be provided to any individuals, regulators, law enforcement agencies, consumer reporting agencies or others as required by law or regulation, or otherwise in the Commonwealth's discretion; and (ii) the contents of such notice, whether any type or remediation may be offered to affected persons, and the nature and extent of any such remediation.

(d)   <u>Diligent Performance and Cooperation.</u> The Licensor shall diligently perform all of the duties required in this Section in cooperation with the Commonwealth.

(e)   The requirements of this section are in addition to and not in lieu of other requirements of this Agreement and its Attachments and Exhibits having to do with data privacy and security, including but not limited to the requirement that the Licensor comply with Attachment 2, *Requirements for Non-Commonwealth Hosting Applications/Services*, and all applicable Commonwealth Information Technology Policies (ITPs), which can be found at: http://www.oa.pa.gov/Policies/Pages/itp.aspx.

17.   **Hyperlink Content.** Any terms and conditions contained in any hyperlink content referenced in this Agreement ("Hyperlink Content") shall not apply to the extent such terms and conditions are expressly prohibited by applicable law. In addition, no financial obligation of the Commonwealth to Licensor shall be affected by any change to information contained in a hyperlink, nor will any additional material obligations be placed on the Commonwealth as a result of any such changes to Hyperlink Content. Terms and conditions in the Hyperlink Content that are materially inconsistent with the Agreement are rejected, unenforceable by the Licensor, and shall not become part of this Agreement unless such terms and conditions are to the benefit of the Commonwealth.

18.   **Publicity/Advertisement**. The Licensor must obtain written Commonwealth approval prior to mentioning the Commonwealth or a Commonwealth Agency in an advertisement, endorsement, or any other type of publicity. This includes the use of any trademark or logo.

19. **Portability**. The parties agree that a Commonwealth Agency may move a Licensed Product from machine to machine, whether physical or virtual, and to other locations, where those machines and locations are internal to the Commonwealth or to a Commonwealth contractor, as long as such relocation and the use being made of the Licensed Product comports with the license grant and restrictions. Notwithstanding the foregoing, a Commonwealth Agency may move the machine or appliance provided by the Licensor upon which the Licensed Product is installed.

20. **Taxes-Federal, State and Local; Interest**.

(a) The Commonwealth is exempt from all excise taxes imposed by the Internal Revenue Service and has accordingly registered with the Internal Revenue Service to make tax-free purchases under registration No. 23-23740001-K. With the exception of purchases of the following items, no exemption certificates are required and none will be issued: undyed diesel fuel, tires, trucks, gas-guzzler emergency vehicles, and sports fishing equipment. The Commonwealth is also exempt from Pennsylvania sales tax, local sales tax, public transportation assistance taxes, and fees and vehicle rental tax. The Department of Revenue regulations provide that exemption certificates are not required for sales made to governmental entities and none will be issued. Nothing in this section is meant to exempt a construction contractor from the payment of any of these taxes or fees which are required to be paid with respect to the purchase, use, rental or lease of tangible personal property or taxable services used or transferred in connection with the performance of a construction contract.

(b) The only interest the Commonwealth is authorized to pay is in accordance with Act of December 13, 1982, P.L. 1155, No. 266, as amended, 72 P. S. § 1507, (relating to Interest Penalties on Commonwealth Accounts) and accompanying regulations 4 Pa. Code §§ 2.31—2.40 (relating to Interest Penalties for Late Payments).

21. **Commonwealth Audit Responsibilities**.

(a) The Commonwealth shall maintain, and promptly provide to the Licensor upon request, accurate records regarding use of the Licensed Products by or for the Commonwealth. If the Commonwealth becomes aware of any unauthorized use of all or any part of the Licensed Products, the Commonwealth shall notify the Licensor promptly, providing reasonable details. The limit of the Commonwealth's responsibility for use of the Licensed Products by more individuals than are permitted by the licensing terms applicable to the Licensed Products shall be to purchase additional licenses and Maintenance and Support (if applicable) for such Licensed Products through a reseller contract or another procurement document.

(b) The Commonwealth shall perform a self-audit upon the request of the Licensor, which request may not occur more often than annually, and report any change in user count (hereinafter "True up number"). The Commonwealth shall notify the

Licensor of the True up number no later than **45 calendar days** after the request that the Commonwealth perform a self-audit. If the user count has increased, the Commonwealth shall make an additional purchase of the Licensed Products through a reseller contract or another procurement document, which is equivalent to the additional users. This section sets out the sole software license audit right under this Agreement.

22. *Right-to-Know Law*. The Pennsylvania *Right-to-Know Law,* Act of February 14, 2008, P.L. 6, No. 3, 65 P.S. §§ 67.101—3104 ("RTKL"), applies to this Agreement.

23. **Third-Party Software**. If a Licensed Product utilizes or includes third party software and other copyrighted material, any additional licensing terms, acknowledgements or disclaimers associated with the third-party software and materials shall not be applicable to the Commonwealth unless agreed to in writing. The parties agree that the Commonwealth, by acknowledging third-party software, does not agree to any terms and conditions of the third-party software agreements.

24. **Attorneys' Fees**. The Commonwealth is not responsible for and shall not pay attorneys' fees incurred by or paid by the Licensor.

25. **Controversies**.

    (a)   Pursuant to Section 1712.1 of the *Commonwealth Procurement Code,* 62 Pa. C.S. § 1712.1, in the event of a claim arising from the Agreement or a purchase order, the Licensor, within **six (6) months** after the claim accrues, must file a written claim with the contracting officer for a determination. The claim shall state all grounds upon which the Licensor asserts a controversy exists. If the Licensor fails to file a claim or files an untimely claim, the Licensor is deemed to have waived its right to assert a claim in any forum. At the time the claim is filed, or within **60 days** thereafter, either party may request mediation through the Commonwealth Office of General Counsel Dispute Resolution Program, http://www.ogc.pa.gov/Services%20to%20Agencies/Mediation%20Procedures/Pages/default.aspx.

    (b)   If the Licensor or the contracting officer requests mediation and the other party agrees, the contracting officer shall promptly make arrangements for mediation. Mediation shall be scheduled so as to not delay the issuance of the final determination beyond the required **120 days** after receipt of the claim if mediation is unsuccessful. If mediation is not agreed to or if resolution is not reached through mediation, the contracting officer shall review timely-filed claims and issue a final determination, in writing, regarding the claim. The final determination shall be issued within **120 days** of the receipt of the claim, unless extended by consent of the contracting officer and the Licensor. The contracting officer shall send his/her written determination to the Licensor. If the contracting officer fails to issue a final determination within the **120 day**s (unless extended by consent of the parties), the

claim shall be deemed denied. The contracting officer's determination shall be the final order of the purchasing agency.

(c)   Within **15 days** of the mailing date of the determination denying a claim or within **135 days** of filing a claim if, no extension is agreed to by the parties, whichever occurs first, the Licensor may file a statement of claim with the Commonwealth Board of Claims. Pending a final judicial resolution of a controversy or claim, the Licensor shall proceed diligently with the performance of the Agreement or purchase order in a manner consistent with the determination of the contracting officer and the Commonwealth shall compensate the Licensor pursuant to the terms of the Agreement, purchase order or other procurement document.

26.   Insurance.

(a)   The Licensor shall maintain at its expense, and require its agents, contractors and subcontractors to procure and maintain, as appropriate, the following types and amounts of insurance issued by companies acceptable to the Commonwealth and authorized to conduct such business under the laws of the Commonwealth:

(i)   Workers' Compensation Insurance for all of the employees engaged in performing Services in accordance with the *Worker's Compensation Act,* the Act of June 2, 1915, P.L. 736, No. 338, reenacted and amended June 21, 1939, P.L. 520, No. 281, as amended, 77 P.S.§§ 101—2708.

(ii)   Commercial general liability insurance providing coverage from claims for damages for personal injury, death (including bodily injury), sickness or disease, accidental death and damage to and property of others, including loss of use resulting from any property damage which may arise from the Licensor's operations under this Agreement, whether such operation be by the Licensor, its agent, contractor or subcontractor, or by anyone directly or indirectly employed by either. The limits of such insurance shall be in an amount not less than $500,000 per person and $2,000,000 per occurrence, personal injury and property damage combined. Such policies shall be occurrence based rather than claims-made policies and shall name the Commonwealth of Pennsylvania as an additional insured, as its interests may appear. The insurance shall not contain any endorsements or any other form designed to limit and restrict any action by the Commonwealth as an additional insured against the insurance coverages in regard to the Services performed for or supplies provided to the Commonwealth.

(iii)   Professional and Technology-Based Services Liability Insurance (insuring against damages and claim expenses as a result of claims arising from any actual or alleged wrongful acts in performing cyber and technology activities) in the amount of $2,000,000, per accident/occurrence/annual aggregate.

(iv)   Technology Products Liability/Professional Liability/Errors & Omissions Insurance in the amount of $2,000,000, per accident/occurrence/annual aggregate, covering the Licensor, its employees, agents, contractors, and subcontractors in the performance of all services.

(v)   Comprehensive crime insurance in an amount of not less than $5,000,000 per claim.

(vi)   Information Security and Privacy Liability Insurance including Privacy Notification Costs (including coverage for Technology Professional Liability if not covered under Licensor's Professional Liability/Errors and Omissions Insurance referenced above) in the amount of $3,000,000, per accident/occurrence/annual aggregate, covering the Licensor, its employees, agents, contractors, and subcontractors in the performance of all services.

(b)   <u>Certificate of Insurance</u>. Prior to providing Licensed Products under this Agreement, and annually thereafter, the Licensor shall provide the Commonwealth with a copy of each current certificate of insurance required by this section. These certificates shall contain a provision that coverages afforded under the policies will not be canceled or changed in such a way to cause the coverage to fail to comply with the requirements of this section until at least **15 days**' prior written notice has been received by the Commonwealth. Such cancellation or change shall not relieve the Licensor of its continuing obligation to maintain insurance coverage in accordance with this section.

(c)   <u>Insurance coverage length</u>. The Licensor shall maintain such insurance for the life of any applicable purchase order issued pursuant to the Agreement.

27. Signatures.

(a)   The parties agree that: (1) a record or signature may not be denied legal effect or enforceability solely because it is in electronic form; (2) a contract may not be denied legal effect or enforceability solely because an electronic record was used in its formation; (3) if a law requires a record to be in writing, an electronic record satisfies the law; and (4) if law requires a signature, an electronic signature satisfies the law.

(b)   The fully executed Agreement may not contain ink signatures by the Commonwealth. If this Agreement does not contain ink signatures by the Commonwealth, the Licensor understands and agrees that the receipt of an electronically-printed Agreement with the printed name of the Commonwealth purchasing agent constitutes a valid, binding contract with the Commonwealth. The printed name of the purchasing agent represents the signature of that individual who is authorized to bind the Commonwealth to the obligations contained in this

Agreement. The printed name also indicates that all approvals required by Commonwealth contracting procedures have been obtained.

28. **Independent Contractor**. The parties are independent contractors, and this Agreement does not create an agency, partnership or joint venture.

29. **Travel**. The Licensor shall not be allowed or paid travel or per diem expenses except as specifically set forth in this Agreement or Statement of Work. If not otherwise specified in the Agreement or Statement of Work, travel and related expenses shall be reimbursed in accordance with Management Directive 230.10 Amended, *Commonwealth Travel Policy*, and Manual 230.1, *Commonwealth Travel Procedures Manual*.

30. **Entire Agreement**. This Agreement constitutes the entire agreement between the parties pertaining to the subject matter hereof, and supersedes and integrates all prior discussions, agreements and understandings pertaining thereto. No modification of this Agreement will be effective unless in writing and signed by both Parties. Other terms and conditions or additional terms and conditions included or referenced in the Licensor's quotations, invoices, business forms, or other documentation shall not become part of the parties' agreement and shall be disregarded by the parties, unenforceable by the Licensor and not binding on the Commonwealth. No modification of this Agreement will be effective unless in writing and signed by both Parties.

31. **Assignment.** Either party may assign this Agreement in its entirety, but not in parts, on written notice to the other party to its parent company, affiliate or subsidiary, in connection with a merger, consolidation, or sale or other disposition of all or substantially all of its assets, or in the case of the Commonwealth to another Commonwealth entity. Any other assignment shall be null and void, except with the other party's prior written consent, which shall not be unreasonably withheld. This Agreement and all obligations shall be binding upon and inure to the benefit of the parties' successors and lawful assignees.

32. **Notice**. Any written notice to either party under this Agreement shall be deemed sufficient if delivered personally, or by facsimile, telecopy, electronic or digital transmission (provided such delivery is confirmed), or by a recognized overnight courier service (e.g., DHL, Federal Express, etc.), with confirmed receipt, or by certified or registered United States mail, postage prepaid, return receipt requested, sent to the address such party may designate by notice given pursuant to this section.

33. **Survival**. The termination or expiration of this Agreement will not affect any provisions of this Agreement which by their nature survive termination or expiration, including the provisions that deal with the following subject matters: definitions, confidentiality, term and termination, effect of termination, intellectual property, license compliance, limitation of liability, indemnification and privacy.

34. **Waiver**. Failure to enforce any provision will not constitute a waiver.

35.   **Severability**. If any provision is found unenforceable, it and any related provisions will be interpreted to best accomplish the unenforceable provision's essential purpose.

36.   **Nonexclusive Remedy**. Except as expressly set forth in this Agreement, the exercise by either party of any of its remedies under this Agreement will be without prejudice to its other remedies under this Agreement or otherwise.

37.   **Integration**. This Agreement, including all exhibits and referenced documents, and any Purchase Orders referencing this Agreement, constitutes the entire agreement between the parties. No agent, representative, employee or officer of the Commonwealth or of Licensor has authority to make any statement, agreement, or representation, oral or written, in connection with this Agreement, which in any way can be deemed to modify, add to, or detract from, or otherwise change or alter its terms and conditions. No negotiations between the parties, nor any custom or usage, shall be permitted to modify or contradict any of the terms and conditions of this Agreement. No modifications, alterations, changes, or waiver to this Agreement or any of its terms shall be valid or binding unless accomplished by a written amendment executed by the parties.

[Reminder of Page Intentionally Left Blank]

The parties to this Agreement have executed it, through their respective duly authorized representatives.

Witness: **Licensor:**

_____   _____
Signature   Date   Signature   Date

_____   _____
Printed Name   Printed Name

_____   _____
Title   Title

If a corporation, the Chairman, President, Vice-President, Senior Vice-President, Executive Vice-President, Assistant Vice-President, Chief Executive Officer or Chief Operating Officer must sign; if a sole proprietor, then the owner must sign; if a general or limited partnership, a general partner must sign; if a limited liability company, then a member must sign, unless it is a managed by a manager, then the manager must sign; otherwise a resolution indicating authority to bind the corporation must be attached to this Agreement.

COMMONWEALTH OF PENNSYLVANIA
GOVERNOR'S OFFICE OF ADMINISTRATION

 Electronically signed per Section 27
Agency Head or Designee

APPROVED AS TO FORM AND LEGALITY:

 Electronically signed per Section 27   **Electronically signed per Section 27**
Office of Chief Counsel   Office of General Counsel

 Electronically signed per Section 27
Office of Attorney General

APPROVED:

 Electronically signed per Section 27
Comptroller

ATTACHMENT 1

LIST OF LICENSED PRODUCTS

With the consent of the Commonwealth, additional Licensed Products may be added to this attachment by Licensor providing the Commonwealth with a new copy of this Attachment 1.

Licensed Products:

The Licensed Products include (list all titles covered by this Agreement):

ATTACHMENT 2

**Requirements for Non-Commonwealth Hosted
Applications/Services**

The purpose of this Attachment is to define requirements for business or technology solutions and services procured by the Commonwealth that are hosted within the Licensor's or its subcontractor's managed infrastructure.

A.   Hosting Requirements

1.   The Licensor or its subcontractor shall supply all hosting equipment (hardware and software) required for the cloud services and performance of the software and services set forth in the Quote and Statement of Work.

2.   The Licensor shall provide secure access to applicable levels of users via the internet.

3.   The Licensor shall use commercially reasonable resources and efforts to maintain adequate internet connection bandwidth and server capacity.

4.   The Licensor or its subcontractors shall maintain all components of the hosted solution with commercially reasonable support and replace as necessary to maintain compliance.

5.   The Licensor shall monitor, prevent and deter unauthorized system access. The Licensor shall use all commercially reasonable methods to confirm suspected breaches. In the event of any impermissible disclosure unauthorized loss or destruction of Confidential Information, the receiving Party must immediately notify the disclosing Party and take all reasonable steps to mitigate any potential harm or further disclosure of such Confidential Information. In addition, pertaining to the unauthorized access, use, release, or disclosure of data, the Licensor shall comply with state and federal data breach notification statutes and regulations, and shall report security incidents to the Commonwealth within **one (1) hour** of when the Licensor has reasonable confirmation of such unauthorized access, use, release, or disclosure of data.

6.   The Licensor or the Licensor's subcontractor shall allow the Commonwealth or its delegate, at times chosen by the Commonwealth, and with at least **three (3) business days'** notice, to review the hosted system's data center locations and security architecture.

7.   The Licensor's employees or subcontractors, who are directly responsible for day-to-day monitoring and maintenance of the hosted system, shall have industry standard certifications applicable to the environment and system architecture used.

8.   The Licensor or the Licensor's subcontractor shall locate servers in a climate-controlled environment. The Licensor or the Licensor's contractor shall house all servers and equipment in an operational environment that meets industry standards including climate control, fire and security hazard detection, electrical needs, and physical security.

9.   The Licensor shall examine applicable system and error logs daily to minimize and predict system problems and initiate appropriate action.

10.   The Licensor shall completely test and apply patches for all third-party software products in the server environment before release.

11.   The Licensor shall provide all Commonwealth data to the Commonwealth, upon request, in a form acceptable to the Commonwealth, at no cost to the Commonwealth.

B.   System and Organization Controls (SOC) Reporting Requirements

1.   Subject to this section and unless otherwise agreed to in writing by the Commonwealth, the Licensor shall, and shall require its subcontractors to, engage, on an annual basis, a CPA certified third-party auditing firm to conduct the following, as applicable:

   (i)   a SOC 1 Type II report with respect to controls used by the Licensor relevant to internal and external procedures and systems that process Commonwealth financial transactions; and

   (ii)   a SOC 2 Type II report with respect to controls used by the Licensor relevant to internal and external procedures and systems that access, process, host or contain Commonwealth Data designated as Class "C" Classified Records or Closed Records, as defined in ITP-SEC019, or in compliance with mandates by federal or state audit requirements and/or policy.

   The Licensor shall receive and review their subcontractor's relevant SOC reports, and the Licensor shall provide the Commonwealth with a Letter of Attestation that includes an analysis of their subcontractor's SOC report.

2.   Unless otherwise agreed to in writing by the Commonwealth, the Licensor's SOC Report(s) shall be provided upon contract execution and annually thereafter. While it is preferable that SOC Reports coincide with Pennsylvania's fiscal year (July 1 through June 30), SOC Reports, at the very least, must cover at least **6 consecutive months** of Pennsylvania's fiscal year.

3.   SOC 2 Type II reports shall address the following:

(i)   Security of Information and Systems;
(ii)   Availability of Information and Systems;
(iii)   Processing Integrity;
(iv)   Confidentiality;
(v)   Privacy; and
(vi)   if applicable, compliance with the laws, regulations standards or policies designed to protect the information identified in ITP-SEC019 or other information identified as protected or Confidential by this Contract or under law.

4.   At the request of the Commonwealth, the Licensor shall, and shall require its subcontractors, as applicable, complete a SOC for Cybersecurity audit in the event:

(i)   repeated non-conformities are identified in any SOC report required by subsection 1; or

(ii)   if the Licensor's business model changes (such as a merger, acquisition, or change sub-contractors, etc.).

The SOC for Cybersecurity report shall detail the controls used by the Licensor or its subcontractor setting forth the description and effectiveness of the Licensor's or subcontractor's cybersecurity risk management program and the policies, processes and controls enacted to achieve each cybersecurity objective.

The Licensor shall provide to the Commonwealth a report of the SOC for Cybersecurity audit findings within **60 days** of its completion.

5.   The Commonwealth may specify other or additional standards, certifications or audits it requires under any Purchase Orders or within an ITP.

6.   The Licensor shall adhere to Statement on Standards for Attestation Engagements (SSAE) 18 audit standards. The Licensor acknowledges that the SSAE guidance may be updated during the Term of this Contract, and the Licensor shall comply with such updates which shall be reflected in the next annual report.

7.   In the event an audit reveals any non-conformity to SSAE standards, the Licensor shall provide the Commonwealth, within **45 days** of the issuance of the SOC report, a documented corrective action plan that addresses each non-conformity that is identified within the SOC report, including any subcontractor's SOC report. The corrective action plan shall provide, in detail:

<blockquote>

(i)   clear responsibilities of the personnel designated to resolve the non-conformity;

(ii)   the remedial action to be taken by the Licensor or its subcontractor(s);

(iii)   the dates when each remedial action is to be implemented; and

(iv)   a summary of potential risks or impacts to the Commonwealth that are associated with the non-conformity(ies).

</blockquote>

8.   The Commonwealth may in its sole discretion agree, in writing, to accept alternative security report in lieu of a SOC report.

C. Security Requirements

1.   The Licensor shall conduct a third-party independent security/vulnerability assessment at its own expense on an annual basis.

2.   The Licensor shall comply with the Commonwealth's directions/resolutions to remediate the results of the security/vulnerability assessment to align with the standards of the Commonwealth.

3.   The Licensor shall use industry best practices to protect access to the system with a firewall and firewall rules to prevent access by non-authorized users and block all improper and unauthorized access attempts.

4.   The Licensor shall use industry best practices to provide applicable system intrusion detection and prevention in order to detect intrusions in a timely manner.

5.   The Licensor shall use industry best practices to provide applicable malware and virus protection or compensating controls on all servers and network components.

6.   The Licensor shall limit access to Commonwealth-specific systems, data and services and provide access only to those staff, located within CONUS (any of the Continental United States and Hawaii) that must have access to provide services proposed.

7.   The Licensor shall provide the services, using security technologies and techniques in accordance with industry best practices and the Commonwealth's ITPs set forth in Attachment 2-A, including those relating to the prevention and detection of intrusions, and any other inappropriate use or access of systems and networks.

D. Data Protection

1.   The Licensor shall only host, store or backup Commonwealth Data in physical locations within CONUS.

2. The Licensor shall use industry best practices to update and patch all applicable systems and third-party software security configurations to reduce security risk.

3. The Licensor shall protect their operational systems with applicable anti-virus, host intrusion protection, incident response monitoring and reporting, network firewalls, application firewalls, and employ system and application patch management to protect its network and customer data from unauthorized disclosure.

4. The Licensor shall be solely responsible for applicable data storage required.

5. The Licensor shall encrypt all Commonwealth data in transit and at rest. The Licensor shall comply with ITP-SEC031, and ITP-SEC019, encryption policies and minimum standards or stronger.

6. The Licensor shall take all commercially viable and applicable measures to protect the data availability including, but not limited to, real-time replication, traditional backup, and/or georedundant storage of Commonwealth data in accordance with industry best practices and encryption techniques.

7. The Licensor shall have appropriate controls in place to protect critical or sensitive data and shall employ stringent policies, procedures, to protect that data particularly in instances where such critical or sensitive data may be stored on a Licensor-controlled or Licensor-owned electronic device.

8. The Licensor shall utilize a secured backup solution to prevent loss of data. Stored backups must be kept in an all-hazards protective storage environment at the primary location and any additional locations where the data is being maintained. All back up data and media shall be encrypted.

E.   Adherence to Policy

1. The Licensor support and problem resolution solution shall provide a means to classify problems as to criticality and impact and with appropriate resolution procedures and escalation process for classification of each problem.

2. The Licensor shall abide by the applicable Commonwealth's Information Technology Policies (ITPs), a list of the most relevant being attached hereto as Attachment 2-A.

3. The Licensor shall comply with all pertinent federal and state privacy regulations.

F.   Closeout

When the purchase order's or other procurement document's term expires or terminates, and a new purchase order or other procurement document has not been issued by a Commonwealth Agency within **60 days** of expiration or termination, or at any other time at the written request of the Commonwealth, the Licensor must promptly return to the Commonwealth all Commonwealth's data (and all copies of this information) that is in the Licensor's possession or control. The Commonwealth's data shall be returned in a format agreed to by the Commonwealth.

Upon confirmation that Commonwealth data is in possession or control of the Commonwealth, the Licensor shall ensure all residual user account(s) are promptly deleted or reset in the solution. The Licensor shall notify the Commonwealth within **10 business days** that all user account(s) have been deleted or reset.

ATTACHMENT 2-A

Information Technology Policies (ITPs) for
Outsourced/Licensor(s)-hosted Solutions

ITP Number - Name	Policy Link
ITP_ACC001 - Accessibility Policy	https://www.oa.pa.gov/Policies/Documents/itp_acc001.pdf
ITP_APP030 - Active Directory Architecture	https://www.oa.pa.gov/Policies/Documents/itp_app030.pdf
ITP_BUS007 - Enterprise Service Catalog	https://www.oa.pa.gov/Policies/Documents/itp_bus007.pdf
ITP_BUS010 - Business Process Management Policy	https://www.oa.pa.gov/Policies/Documents/itp_bus010.pdf
ITP_BUS012 -Artificial Intelligence General Policy	httpss://www.oa.pa.gov/Policies/Documents/itp_bus012.pdf
ITP_INF000 - Enterprise Data and Information Management Policy	https://www.oa.pa.gov/Policies/Documents/itp_inf000.pdf
ITP_INF001 - Database Management Systems	https://www.oa.pa.gov/Policies/Documents/itp_inf001.pdf
ITP_INF006 - Commonwealth County Code Standard	https://www.oa.pa.gov/Policies/Documents/itp_inf006.pdf
ITP_INF009 - e-Discovery Technology Standard	https://www.oa.pa.gov/Policies/Documents/itp_inf009.pdf
ITP_INF010 - Business Intelligence Policy	https://www.oa.pa.gov/Policies/Documents/itp_inf010.pdf
ITP_INF011 - Reporting Policy	https://www.oa.pa.gov/Policies/Documents/itp_inf011.pdf
ITP_INF012 - Dashboard Policy	https://www.oa.pa.gov/Policies/Documents/itp_inf012.pdf
ITP_INFRM001 - The Life Cycle of Records: General Policy Statement	https://www.oa.pa.gov/Policies/Documents/itp_infrm001.pdf
ITP_INFRM004 - Management of Web Records	https://www.oa.pa.gov/Policies/Documents/itp_infrm004.pdf
ITP_INFRM005 - System Design Review of Electronic Systems	https://www.oa.pa.gov/Policies/Documents/itp_infrm005.pdf
ITP_INFRM006 - Electronic Document Management Systems	https://www.oa.pa.gov/Policies/Documents/itp_infrm006.pdf
ITP_INT_B_1 - Electronic Commerce Formats and Standards	https://www.oa.pa.gov/Policies/Documents/itp_int_b_1.pdf
ITP_INT_B_2 - Electronic Commerce Interface Guidelines	https://www.oa.pa.gov/Policies/Documents/itp_int_b_2.pdf
ITP_INT006 - Business Engine Rules	https://www.oa.pa.gov/Policies/Documents/itp_int006.pdf
ITP_NET004 - Internet Protocol Address Standards	https://www.oa.pa.gov/Policies/Documents/itp_net004.pdf
ITP_NET005 - Commonwealth External and Internal Domain Name Services (DNS)	https://www.oa.pa.gov/Policies/Documents/itp_net005.pdf
ITP_PRV001 - Commonwealth of Pennsylvania Electronic Information Privacy Policy	https://www.oa.pa.gov/Policies/Documents/itp_prv001.pdf
ITP_SEC000 - Information Security Policy	https://www.oa.pa.gov/Policies/Documents/itp_sec000.pdf
ITP_SEC001 - Enterprise Host Security Software Policy	httpss://www.oa.pa.gov/Policies/Documents/itp_sec001.pdf
ITP_SEC002 - Internet Accessible Proxy Servers and Services	https://www.oa.pa.gov/Policies/Documents/itp_sec002.pdf
ITP_SEC003 - Enterprise Security Auditing and Monitoring	https://www.oa.pa.gov/Policies/Documents/itp_sec003.pdf
ITP_SEC004 - Enterprise Web Application Firewall	https://www.oa.pa.gov/Policies/Documents/itp_sec004.pdf
ITP_SEC006 - Commonwealth of Pennsylvania Electronic Signature Policy	https://www.oa.pa.gov/Policies/Documents/itp_sec006.pdf
ITP_SEC007 - Minimum Standards for IDs, Passwords and Multi-Factor Authentication	https://www.oa.pa.gov/Policies/Documents/itp_sec007.pdf
ITP_SEC008 - Enterprise E-mail Encryption	https://www.oa.pa.gov/Policies/Documents/itp_sec008.pdf
ITP_SEC009 - Minimum Contractor Background Checks Policy	https://www.oa.pa.gov/Policies/Documents/itp_sec009.pdf
ITP_SEC010 - Virtual Private Network Standards	https://www.oa.pa.gov/Policies/Documents/itp_sec010.pdf

ITP Number - Name	Policy Link
ITP_SEC011 - Enterprise Policy and Software Standards for Agency Firewalls	https://www.oa.pa.gov/Policies/Documents/itp_sec011.pdf
ITP_SEC012 - System Logon Banner and Screensaver Requirements	httpss://www.oa.pa.gov/Policies/Documents/itp_sec012.pdf
ITP_SEC015 - Data Cleansing	https://www.oa.pa.gov/Policies/Documents/itp_sec015.pdf
ITP_SEC016 - Information Security Officer Policy	httpss://www.oa.pa.gov/Policies/Documents/itp_sec016.pdf
ITP_SEC017 - Copa Policy for Credit Card Use for e-Government	https://www.oa.pa.gov/Policies/Documents/itp_sec017.pdf
ITP_SEC019 - Policy and Procedures for Protecting Commonwealth Electronic Data	https://www.oa.pa.gov/Policies/Documents/itp_sec019.pdf
ITP_SEC021 - Security Information and Event Management Policy	https://www.oa.pa.gov/Policies/Documents/itp_sec021.pdf
ITP_SEC023 - Information Technology Security Assessment and Testing Policy	https://www.oa.pa.gov/Policies/Documents/itp_sec023.pdf
ITP_SEC024 - IT Security Incident Reporting Policy	https://www.oa.pa.gov/Policies/Documents/itp_sec024.pdf
ITP_SEC025 - Proper Use and Disclosure of Personally Identifiable Information (PII)	https://www.oa.pa.gov/Policies/Documents/itp_sec025.pdf
ITP_SEC029 - Physical Security Policy for IT Resources	https://www.oa.pa.gov/Policies/Documents/itp_sec029.pdf
ITP_SEC031 - Encryption Standards	https://www.oa.pa.gov/Policies/Documents/itp_sec031.pdf
ITP_SEC032 - Enterprise Data Loss Prevention (DLP) Compliance Standards	https://www.oa.pa.gov/Policies/Documents/itp_sec032.pdf
ITP_SEC034- Enterprise Firewall Rule Set	https://www.oa.pa.gov/Policies/Documents/itp_sec034.pdf
ITP_SEC035 - Mobile Device Security Policy	httpss://www.oa.pa.gov/Policies/Documents/itp_sec035.pdf
ITP_SEC038 - Commonwealth Data Center Privileged User IAM Policy	https://www.oa.pa.gov/Policies/Documents/itp_sec038.pdf
ITP-SEC039 - Keystone Login and Identity Proofing	https://www.oa.pa.gov/Policies/Documents/itp-sec039.pdf
ITP_SEC040 - Commonwealth Cloud Computing Services Requirements	https://www.oa.pa.gov/Policies/Documents/itp_sec040.pdf
ITP SFT000 - Software Development Life Cycle (SDLC) Policy	https://www.oa.pa.gov/Policies/Documents/itp_sft000.pdf
ITP_SFT001 - Software Licensing	https://www.oa.pa.gov/Policies/Documents/itp_sft001.pdf
ITP_SFT002 - Commonwealth of PA Website Standards	https://www.oa.pa.gov/Policies/Documents/itp_sft002.pdf
ITP_SFT003 - Geospatial Enterprise Service Architecture	https://www.oa.pa.gov/Policies/Documents/itp_sft003.pdf
ITP_SFT004 - Geospatial Information Systems (GIS)	https://www.oa.pa.gov/Policies/Documents/itp_sft004.pdf
ITP_SFT005 - Managed File Transfer (MFT)	https://www.oa.pa.gov/Policies/Documents/itp_sft005.pdf
ITP_SFT007 - Office Productivity Policy	https://www.oa.pa.gov/Policies/Documents/itp_sft007.pdf
ITP SFT008 - Enterprise Resource Planning (ERP) Management	https://www.oa.pa.gov/Policies/Documents/itp_sft008.pdf
ITP SFT009 - Application Development	https://www.oa.pa.gov/Policies/Documents/itp_sft009.pdf
ITP_SYM003 - Off-Site Storage for Commonwealth Agencies	https://www.oa.pa.gov/Policies/Documents/itp_sym003.pdf
ITP_SYM004 - Policy for Establishing Alternate Processing Sites for Commonwealth Agencies	https://www.oa.pa.gov/Policies/Documents/itp_sym004.pdf
ITP_SYM006 - Commonwealth IT Resources Patching Policy	https://www.oa.pa.gov/Policies/Documents/itp_sym006.pdf
ITP_SYM008 - Server Virtualization Policy	https://www.oa.pa.gov/Policies/Documents/itp_sym008.pdf
ITP_SYM010 - Enterprise Services Maintenance Scheduling	https://www.oa.pa.gov/Policies/Documents/itp_sym010.pdf

COMMONWEALTH OF PENNSYLVANIA
SAMPLE **BUSINESS ASSOCIATE AGREEMENT**
(Business Associate Agreements as provided by Agencies may differ)

WHEREAS, the _____ (Covered Entity) and _____ (Business Associate) intend to protect the privacy and security of certain Protected Health Information (PHI) to which Business Associate may have access in order to provide goods or services to or on behalf of Covered Entity, in accordance with the *Health Insurance Portability and Accountability Act of 1996*, as amended, Pub. L. No. 104-191 (HIPAA), the *Health Information Technology for Economic and Clinical Health (HITECH) Act*, as amended, Title XIII of Division A and Title IV of Division B of the *American Recovery and Reinvestment Act of 2009* (ARRA), as amended, Pub. L. No. 111-5 (Feb. 17, 2009) and related regulations, the HIPAA Privacy Rule (Privacy Rule), 45 C.F.R. Parts 160 and 164, as amended, the HIPAA Security Rule (Security Rule), 45 C.F.R. Parts 160, 162 and 164), as amended, 42 C.F.R. §§ 431.301—431.302, 42 C.F.R. Part 2, 45 C.F.R. § 205.50, 42 U.S.C. § 602(a)(1)(A)(iv), 42 U.S.C. § 1396a(a)(7), 35 P.S. § 7607, 50 Pa. C.S. § 7111, 71 P.S. § 1690.108(c), 62 P.S. § 404, 55 Pa. Code Chapter 105, 55 Pa. Code Chapter 5100, the Pennsylvania *Breach of Personal Information Notification Act*, Act of December 22, 2005, P.L. 474, No. 94, as amended, 73 P.S. §§ 2301—2329, and other relevant laws, including subsequently adopted provisions applicable to use and disclosure of confidential information, and applicable agency guidance; and,

WHEREAS, Business Associate may receive PHI from Covered Entity, or may create or obtain PHI from other parties for use on behalf of Covered Entity, which PHI may be used or disclosed only in accordance with this Agreement and the standards established by applicable laws and agency guidance; and

WHEREAS, Business Associate may receive PHI from Covered Entity, or may create or obtain PHI from other parties for use on behalf of Covered Entity, which PHI must be handled in accordance with this Agreement and the standards established by HIPAA, the HITECH Act and related regulations, the Privacy Rule, the Security Rule and other applicable laws and agency guidance.

NOW, THEREFORE, Covered Entity and Business Associate agree as follows:

1.   **Definitions**.

    (a)   "**Business Associate**" shall have the meaning given to such term under HIPAA, the HITECH Act and related regulations, the Privacy Rule, the Security Rule and agency guidance.

    (b)   "**Covered Entity**" shall have the meaning given to such term under HIPAA, the HITECH Act and related regulations, the Privacy Rule, the Security Rule and agency guidance.

(c)   "**HIPAA**" shall mean the *Health Insurance Portability and Accountability Act of 1996*, as amended, Pub. L. No. 104-191.

(d)   "**HITECH Act**" shall mean the *Health Information Technology for Economic and Clinical Health (HITECH) Act*, as amended, Title XIII of Division A and Title IV of Division B of the American Recovery and Reinvestment Act of 2009 (ARRA), Pub. L. No. 111-5 (Feb. 17, 2009).

(e)   "**Privacy Rule**" shall mean the standards for privacy of individually identifiable health information in 45 C.F.R. Parts 160 and 164, as amended, and related agency guidance.

(f)   "**Protected Health Information**" or "**PHI**" shall have the meaning given to such term under HIPAA, the HITECH Act and related regulations, the Privacy Rule, the Security Rule (all as amended) and agency guidance.

(g)   "**Security Rule**" shall mean the security standards in 45 C.F.R. Parts 160, 162 and 164, as amended, and related agency guidance.

(h)   "**Unsecured PHI**" shall mean PHI that is not secured through the use of a technology or methodology as specified in HITECH Act regulations, as amended, and agency guidance or as otherwise defined in the HITECH Act, as amended.

2.   **Stated Purposes for Which Business Associate May Use or Disclose PHI**. The Parties hereby agree that Business Associate shall be permitted to use and/or disclose PHI provided by or obtained on behalf of Covered Entity for the following stated purposes, except as otherwise stated in this Agreement:

_____
_____
_____
_____
_____
_____
_____
_____
_____

NO OTHER DISCLOSURES OF PHI OR OTHER INFORMATION ARE PERMITTED.

3.   **BUSINESS ASSOCIATE OBLIGATIONS**.

(a)   **Limits on Use and Further Disclosure**. Business Associate shall not further use or disclose PHI provided by, or created or obtained on behalf of, Covered Entity

other than as permitted or required by this Addendum, as requested by Covered Entity, or as required by law and agency guidance.

(b) **Appropriate Safeguards**. Business Associate shall establish and maintain appropriate safeguards to prevent any use or disclosure of PHI other than as provided for by this Agreement. Appropriate safeguards shall include implementing administrative, physical and technical safeguards that reasonably and appropriately protect the confidentiality, integrity and availability of the electronic PHI that is created, received, maintained or transmitted on behalf of the Covered Entity and limiting use and disclosure to applicable minimum necessary requirements as set forth in applicable federal and state statutory and regulatory requirements and agency guidance.

(c) **Reports of Improper Use or Disclosure**. Business Associate hereby agrees that it shall report to _____at _____, within **two (2) days** of discovery any use or disclosure of PHI not provided for or allowed by this Agreement.

(d) **Reports on Security Incidents**. In addition to following the breach notification requirements in section 13402 of the *Health Information Technology for Economic and Clinical Health Act of 2009* ("HITECH Act"), as amended, and related regulations, the Privacy Rule, the Security Rule, agency guidance and other applicable federal and state laws, Business Associate shall report to _____at _____, **within two (2) days** of discovery any security incident of which it becomes aware. At the sole expense of Business Associate, Business Associate shall comply with all federal and state breach notification requirements, including those applicable to Business Associate and those applicable to Covered Entity. Business Associate shall indemnify the Covered Entity for costs associated with any incident involving the acquisition, access, use or disclosure of Unsecured PHI in a manner not permitted under federal or state law and agency guidance. For purposes of the security incident reporting requirement, inconsequential unsuccessful incidents that occur on a daily basis, such as scans, "pings," or other unsuccessful attempts to penetrate computer networks or servers containing electronic PHI maintained by Business Associate, need not be reported in accordance with this section, but may instead be reported in the aggregate on a monthly basis.

(e) **Subcontractors and Agents**. At any time PHI is provided or made available to Business Associate subcontractors or agents, Business Associate shall provide only the minimum necessary PHI for the purpose of the covered transaction and shall first enter into a subcontract or contract with the subcontractor or agent that contains substantially the same terms, conditions and restrictions on the use and disclosure of PHI as contained in this Agreement.

(f) **Right of Access to PHI**. Business Associate shall allow, for any PHI maintained in a designated record set, Covered Entity to have access to and copy an individual's

PHI within **five (5) business days** of receiving a written request from the Covered Entity. Business Associate shall provide PHI in the format requested, if it is readily producible in such form and format; or if not, in a readable hard copy form or such other form and format as agreed to by Business Associate and the individual. If the request is for information maintained in one or more designated record sets electronically and if the individual requests an electronic copy of such information, Business Associate must provide Covered Entity with access to the PHI in the electronic form and format requested by the individual, if it is readily producible in such form and format; or, if not, in a readable electronic form and format as agreed to by the Business Associate and Covered Entity. If any individual requests from Business Associate or its agents or subcontractors access to PHI, Business Associate shall notify Covered Entity within **five (5) business days**. Business Associate shall further conform with all of the requirements of 45 C.F.R. § 164.524 and other applicable laws, including the HITECH Act, as amended, related regulations and agency guidance. Business Associate shall indemnify Covered Entity for costs/damages associated with Business Associate's failure to respond within the time frames set forth in this subsection 3(f).

(g) **Amendment and Incorporation of Amendments**. Within **five (5) business days** of receiving a written request from Covered Entity for an amendment of PHI maintained in a designated record set, Business Associate shall make the PHI available and incorporate the amendment to enable Covered Entity to comply with 45 C.F.R. § 164.526, applicable federal and state law, including the HITECH Act , as amended and related regulations, the Privacy Rule, the Security Rule and agency guidance. If any individual requests an amendment from Business Associate or its agents or subcontractors, Business Associate shall notify Covered Entity within **five (5) business days**.

(h) **Provide Accounting of Disclosures**. Business Associate shall maintain a record of all disclosures of PHI made by Business Associate which are not excepted from disclosure accounting requirements under HIPAA, HITECH and related regulations, the Privacy Rule or the Security Rule (all as amended) in accordance with 45 C.F.R. § 164.528 and other applicable laws and agency guidance, including the HITECH Act and related regulations. Such records shall include, for each disclosure, the date of the disclosure, the name and address of the recipient of the PHI, a description of the PHI disclosed, the name of the individual who is the subject of the PHI disclosed, and the purpose of the disclosure. Business Associate shall make such record available to the Covered Entity within **five (5) business days** of a written request for an accounting of disclosures. Business Associate shall indemnify Covered Entity for costs/damages associated with Business Associate's failure to respond within the time frames set forth in this subsection 3(h).

(i) **Requests for Restriction**. Business Associate shall comply with requests for restrictions on disclosures of PHI about an individual if the disclosure is to a health plan for purposes of carrying out payment or health care operations (and is not for treatment purposes), and the PHI pertains solely to a health care item or service for

which the service involved was paid in full out-of-pocket. For other requests for restriction, Business associate shall otherwise comply with the Privacy Rule, as amended, and other applicable statutory and regulatory requirements and agency guidance.

(j) **Access to Books and Records**. Business Associate shall make its internal practices, books and records relating to the use or disclosure of PHI received from, or created or received, by Business Associate on behalf of the Covered Entity, available to the Secretary of Health and Human Services or designee for purposes of determining compliance with applicable laws and agency guidance.

(k) **Return or Destruction of PHI**. At termination of this Agreement, Business Associate hereby agrees to return or destroy all PHI provided by or obtained on behalf of Covered Entity. Business Associate agrees not to retain any copies of the PHI after termination of this Agreement. If return or destruction of the PHI is not feasible, Business Associate agrees to extend the protections of this Agreement to limit any further use or disclosure until such time as the PHI may be returned or destroyed. If Business Associate elects to destroy the PHI, it shall certify to Covered Entity that the PHI has been destroyed.

(l) **Maintenance of PHI**. Notwithstanding subsection 3(k) of this Agreement, Business Associate and its subcontractors or agents shall retain all PHI throughout the term of the Agreement and shall continue to maintain the information required under the various documentation requirements of this Agreement (such as those in subsection 3(h)) for a period of **six (6) years** after termination of the Agreement, unless Covered Entity and Business Associate agree otherwise.

(m) **Mitigation Procedures**. Business Associate agrees to establish and to provide to Covered Entity upon request, procedures for mitigating, to the maximum extent practicable, any harmful effect from the use or disclosure of PHI in a manner contrary to this Agreement or the Privacy Rule, as amended. Business Associate further agrees to mitigate any harmful effect that is known to Business Associate of a use or disclosure of PHI by Business Associate in violation of this Agreement or applicable laws and agency guidance.

(n) **Sanction Procedures**. Business Associate agrees that it shall develop and implement a system of sanctions for any employee, subcontractor or agent who violates this Agreement, applicable laws or agency guidance.

(o) **Grounds for Breach**. Non-compliance by Business Associate with this Agreement or the Privacy or Security Rules, as amended, is a breach of the Agreement, if Business Associate knew or reasonably should have known of such non-compliance and failed to immediately take reasonable steps to cure the non-compliance. Commonwealth may elect to terminate Business Associate's contract for such breach.

(p)   **Termination by Commonwealth**. Business Associate authorizes termination of this Agreement by the Commonwealth if the Commonwealth determines, in its sole discretion, that the Business Associate has violated a material term of this Agreement.

(q)   **Failure to Perform Obligations**. In the event Business Associate fails to perform its obligations under this Agreement, Covered Entity may immediately discontinue providing PHI to Business Associate. Covered Entity may also, at its option, require Business Associate to submit to a plan of compliance, including monitoring by Covered Entity and reporting by Business Associate, as Covered Entity in its sole discretion determines to be necessary to maintain compliance with this Agreement and applicable laws and agency guidance.

(r)   **Privacy Practices**. Covered Entity will provide Business Associate with all applicable forms, including but not limited to, any form used for Notice of Privacy Practices, Accounting for Disclosures, or Authorization, upon the effective date designated by the Program or Covered Entity. Covered Entity may change applicable privacy practices, documents and forms. The Business Associate shall make reasonable endeavors to implement changes as soon as practicable, but not later than **45 days** from the date of notice of the change. Business Associate shall otherwise comply with all applicable laws and agency guidance pertaining to notices of privacy practices, including the requirements set forth in 45 C.F.R. § 164.520.

4.   **OBLIGATIONS OF COVERED ENTITY**.

(a)   **Provision of Notice of Privacy Practices**. Covered Entity shall provide Business Associate with the notice of privacy practices that the Covered Entity produces in accordance with applicable law and agency guidance, as well as changes to such notice. Covered Entity will post on its website any material changes to its notice of privacy practices by the effective date of the material change.

(b)   **Permissions**. Covered Entity shall provide Business Associate with any changes in, or revocation of, permission by individual to use or disclose PHI of which Covered Entity is aware if such changes affect Business Associate's permitted or required uses and disclosures.

(c)   **Restrictions**. Covered Entity shall notify Business Associate in writing of any restriction to the use or disclosure of PHI that the Covered Entity has agreed to in accordance with 45 C.F.R. § 164.522, as amended, and other applicable laws and applicable agency guidance, to the extent that such restriction may affect Business Associate's use or disclosure of PHI.

(d)   **Requests**. Covered Entity shall not request Business Associate to use or disclose PHI in any manner that would not be permissible under HIPAA, HITECH and

related regulations, the Privacy Rule or the Security Rule, all as amended, if done by Covered Entity.

5. **MISCELLANEOUS**.

    (a) **Regulatory References**. A reference in this Addendum to a section in HIPAA, HITECH and related regulations, the Privacy Rule or the Security Rule refers to the most current version of the section in effect or as amended.

    (b) **Amendment**. The parties agree to take such action as is necessary to amend this Addendum from time to time in order to ensure compliance with the requirements of the HIPAA, HITECH and related regulations, the Privacy Rule, the Security Rule and any other applicable law, all as amended.

    (c) **Conflicts**. In the event that any terms of this Agreement are inconsistent with the terms of the Agreement, then the terms of this Agreement shall control.

Attachment 4

Sign-Off Document No. ____, under Agreement No. _____
Between
[Licensor_____], and the Commonwealth of PA, [Agency]

[Licensor_____] Agency-level Deployment

This document becomes, upon its execution by the signatories named below, a legally valid, binding part of Software/Services License Requirements Agreement No. _____ between the Commonwealth and _____(Licensor) and is subject to the terms of that Agreement.

Scope of Deployment (need not be entire agency):

Nature of Data implicated or potentially implicated:

Agency Policies to which Licensor. is subject (incorporated by reference):

Background checks (describe if necessary):

Additional requirements (describe with specificity):

Is Licensor. a Business Associate (yes or no)?

If yes, the attached Business Associates Agreement, as completed by the Agency, is applicable and is hereby incorporated into this Sign-Off Document by reference.

Agency Contact Person signature and Date: _____

[Licensor_____]
Authorized Signatory and Date: _____