APPENDIX A
ADDITIONAL CONTRACT TERMS AND CONDITIONS

1. **Disclosure of Recipient or Beneficiary Information Prohibited**. The Supplier shall not use or disclose any information about a recipient receiving services from, or otherwise enrolled in, a Commonwealth program affected by or benefiting from Services under the Contract for any purpose not connected with the Supplier's responsibilities, except with consent pursuant to applicable law or regulations. All material associated with direct disclosures of this kind (including the disclosed information) shall be provided to the Commonwealth prior to the direct disclosure.

2. **Compliance with Laws**. Supplier will comply with all applicable laws or regulations related to the use and disclosure of information, including information that constitutes Protected Health Information (PHI) as defined by the *Health Insurance Portability and Accountability* Act (HIPAA).

   Further, by signing this Contract, the Supplier agrees to the terms of the Business Associate Agreement, which is incorporated into this Contract as **Appendix B**, or as otherwise negotiated by the Supplier and the purchasing agency. It is understood that **Appendix B - *Commonwealth of Pennsylvania Business Associate Agreement***, is only applicable if and to the extent indicated in the Contract.

3. **Additional Provisions**. Additional privacy and confidentiality requirements may be specified in the Contract.

4. **Restrictions on Use**. All Data and all intellectual property provided to the Supplier pursuant to this Contract or collected or generated by the Supplier on behalf of the Commonwealth pursuant to this Contract shall be used only for the work of this Contract. No Data, intellectual property, Documentation or Developed Works may be used, disclosed, or otherwise opened for access by or to the Supplier or any third party unless directly related to and necessary under the Contract.

5. **Health Insurance Portability and Accountability Act (HIPAA) Regulations.** The supplier will comply with all federal or state laws related to the use and disclosure of information, including information that constitutes Protected Health Information (PHI) as defined by the Health Insurance Portability and Accountability Act (HIPAA).

   The supplier will be responsible to present to the DOC (BHCS) a detailed action plan to ensure compliance with HIPAA regulations and assist the DOC in planning, developing, and adhering to HIPAA requirements, as DOC deems necessary.

   The supplier will be responsible for assessing its obligations pursuant to HIPAA and will include such assessment in its technical proposal. The supplier will be required to execute the **Business Associates Agreement** contained in **Appendix B**.

6. **Insurance**. The Commonwealth of Pennsylvania will not provide any insurance coverage to the supplier, its employees or subcontractors. The supplier shall obtain and maintain the following insurance covering the supplier and those employees of the supplier providing any service under this Contract:

a. Commercial Automobile Liability Insurance: Automobile insurance is not necessary unless the selected Supplier, the selected Supplier's employees, or subcontractors will be driving on state property or will be using, owned, hired, or non-owned vehicles to conduct business on behalf of the selected Supplier.

The selected Supplier will maintain insurance protecting it from claims for damages from bodily injury as well as from claims for property damage resulting from the ownership, operation, maintenance or use of all owned, hired, and non-owned autos which may arise from operations under the Contract, and in case any work is subcontracted the selected Supplier will require to maintain Commercial Automobile Liability Insurance.

The insurance minimums are as follows:

- $1,000,000 per occurrence combined single limit for Bodily Injury and Property Damage

In addition, the following coverages should be included:

- Owned, Hired, and Non-Owned Automobile.

The following coverages must be included:

- Premises and Operations Bodily Injury and Property Damage;
- Personal and Advertising Injury;
- Blanket Contractual Liability;
- Products and Completed Operations Liability; and
- The DOC named as an additional insured

b. Professional Liability:

- Professional liability insurance in the amount of $1,000,000 per occurrence or claims made, covering the selected Supplier, its employees, agents, contractors and subcontractors in the performance of all services.

c. Additional Insurance Conditions:

- If the supplier receives a cancellation notice from an insurance carrier affording coverage herein, the supplier will notify the DOC within five (5) business days with a copy of the cancellation notice. In such event, the supplier shall obtain alternate coverage to prevent any lapse in required insurance coverage and shall provide the DOC with proof of such coverage.
- The supplier is responsible for payment of Contract related insurance premiums and deductibles.
- If the supplier is self-insured, a Certificate of Self-Insurance must be attached.
- The supplier's policies shall include legal defense fees in addition to its liability policy limits.
- The supplier will obtain insurance policy(ies) from insurance company(ies) having an "AM BEST" rating of A-; Financial Size Category (FSC) VII or better and authorized to do business in the state of Pennsylvania.
- An Umbrella or Excess Liability Insurance Policy may be used to supplement the supplier's policy limits to satisfy the full policy limits required by the Contract.

- The DOC reserves the right to immediately terminate the Contract if the supplier is not in compliance with the insurance requirements and retains all rights to pursue any legal remedies against the supplier. All insurance policies must be open to inspection by the DOC, and copies of policies must be submitted to the DOC's authorized representative upon written request.

Provide a copy of the Offeror's current certificate of insurance which, at a minimum should include the following:

1. Carrier (name and address);
2. Type of insurance;
3. Amount of coverage;
4. Period covered by insurance; and 5. Exclusions.

7. **Information Technology Policies**

a. **General.** The Supplier shall comply with the IT standards and policies issued by the Governor's Office of Administration, Office for Information Technology (located at http://www.oa.pa.gov/Policies/Pages/itp.aspx), including the accessibility standards set out in IT Policy ACC001, Accessibility Policy. The Supplier shall ensure that services and supplies procured under the Contract comply with the applicable standards. In the event such standards change during the Supplier's performance, and the Commonwealth requests that the Supplier comply with the changed standard, then any incremental costs incurred by the Supplier to comply with such changes shall be paid for pursuant to a change order to the Contract.

b. **Waiver.** The Supplier may request a waiver from an ITP by providing detailed written justification as to why the ITP cannot be met. The Commonwealth may waive the ITP in whole, in part, or conditionally, or require that the Supplier provide an acceptable alternative. Any Commonwealth waiver of the requirement must be in writing.

8. **Data Breach or Loss**

a. Supplier shall apply 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*, Act of December 22, 2005, P.L. 474, No. 94, as amended, 73 P.S. §§ 2301—2329.

b. For data and confidential information in the possession, custody, and control of the Supplier or its employees, agents and/or subcontractors:

i. The Supplier shall report unauthorized access, use, release, loss, destruction or disclosure of data or confidential information ("Incident") to the Commonwealth within **two (2) hours** of when the Supplier knows of or reasonably suspects such Incident, and the Supplier must immediately take all reasonable steps to mitigate any potential harm or further access, use, release, loss, destruction or disclosure of such data or confidential information.

ii. Supplier 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, Supplier shall, at its sole expense,

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

iii. Supplier shall be solely responsible for any costs, losses, fines, or damages incurred by the Commonwealth due to Incidents.

c. As to data and confidential information fully or partially in the possession, custody, or control of the Supplier and the Commonwealth, the Supplier shall diligently perform all of the duties required in this Section in cooperation with the Commonwealth, until a time at which a determination of responsibility for the Incident, and for subsequent action regarding the Incident, is made final.

9. **Virus, Malicious, Mischievous or Destructive Programming**

a. The Supplier shall be liable for any damages incurred by the Commonwealth if the Supplier or any of its employees, subcontractors or consultants introduces a virus or malicious, mischievous or destructive programming into the Commonwealth's software or computer networks and has failed to comply with the Commonwealth software security standards. The Commonwealth must demonstrate that the Supplier or any of its employees, subcontractors or consultants introduces the virus or malicious, mischievous or destructive programming. The Supplier's liability shall cease of the Commonwealth has not fully complied with its own software security standards.

b. The Supplier shall be liable for any damages incurred by the Commonwealth including, but not limited to, the expenditure of Commonwealth funds to eliminate or remove a computer virus or malicious, mischievous or destructive programming that results from the Supplier's failure to take proactive measures to keep virus or malicious, mischievous or destructive programming from originating from the Supplier or any of its employees, subcontractors or consultants through appropriate firewalls and maintenance of anti-virus software and software security updates (such as operating systems security patches, etc.).

c. In the event of destruction or modification of software, the Supplier shall eliminate the virus, malicious or mischievous or destructive programming, restore the Commonwealth's software, and be liable to the Commonwealth for any resulting damages.

d. The Supplier shall be responsible for reviewing Commonwealth software security standards and complying with those standards.

e. The Commonwealth may, at any time, audit, by a means deemed appropriate by the Commonwealth, any computing devices being used by representatives of the Supplier to provide services to the Commonwealth for the sole purpose of determining whether those devices have anti-virus software with current virus signature files and the current minimum operating system patches or workarounds have been installed. Devices found to be out of compliance will immediately be disconnected and will not be permitted to connect or reconnect to the Commonwealth network until the proper installations have been made.

f. The Supplier may use the anti-virus software used by the Commonwealth to protect Supplier's computing devices used in the course of providing services to the Commonwealth. It is understood that the Supplier may not install the software on any computing device not being used to provide

services to the Commonwealth, and that all copies of the software will be removed from all devices upon termination of this Contract.

g. The Commonwealth will not be responsible for any damages to the Supplier's computers, data, software, etc. caused a s result of the installation of the Commonwealth's anti-virus software or monitoring software on the Supplier's computers.

10. **Location, Status and Disposition of Data**

a. Unless the ITQ specifies otherwise,

i. All data must be stored within the United States;

ii. The Supplier shall be responsible for maintaining the privacy, security and integrity of Data in the Supplier's or its subcontractors' possession;

iii. All Data shall be provided to the Commonwealth upon request, in a form acceptable to the Commonwealth and at no cost;

iv. Any data shall be destroyed by the Supplier at the Commonwealth's request; and

v. Any data shall be held for litigation or public records purposes by the Supplier at the Commonwealth's request, and in accordance with the security, privacy and accessibility requirements of this Contract.