APPENDIX J

Requirements for non-Commonwealth Hosted Applications/Services

The purpose of this appendix is to define requirements for technology solutions procured by the Commonwealth that are not hosted within Commonwealth infrastructure.

A. Hosting Requirements

1. The selected Offeror shall supply all hosting equipment (hardware and software) required for performance of the Contract.

2. The selected Offeror shall provide secure access to all levels of users via the internet.

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

4. The selected Offeror shall maintain all hosting equipment (hardware and software) and replace as necessary to maintain compliance with the Performance Standards.

5. The selected Offeror shall monitor, prevent and deter unauthorized system access. Any and all known attempts must be reported to the Commonwealth within the timeframe set out by the RFP. In the event of any impermissible disclosure, 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, loss or destruction of such Confidential Information. In addition, pertaining to the unauthorized access, use, release, or disclosure of data, the Provider shall comply with state and federal data breach notifications regulations and is to report security incidents to the Commonwealth within one (1) hour of when the Provider knew of such unauthorized access, use, release, or disclosure of data.

6. The selected Offeror shall allow the Commonwealth or its delegate, at times chosen by the Commonwealth, to review the hosted system's location and security architecture.

7. The selected Offeror staff, directly responsible for day-to-day monitoring and maintenance, shall have industry standard certifications applicable to the environment and system architecture used.

8. The selected Offeror shall locate servers in a climate-controlled environment. Offeror 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 selected Offeror shall examine system and error logs daily to minimize and predict system problems and initiate appropriate action.

10. The selected Offeror shall completely test and apply patches for all third-party software products before release.

B. System Availability

1. The selected Offeror shall make available the system and any custom software on a 24 x 7 basis as established by the RFP.

2. The selected Offeror shall perform routine maintenance during the planned weekly maintenance period. Routine maintenance shall include, but is not limited to, server upgrades/patching, software upgrades/patching and hardware maintenance. In order to maintain system availability, the Offeror is expected to rollover to a backup site during maintenance periods.

3. The selected Offeror shall perform non-routine maintenance at a mutually agreeable time with two (2) weeks advance notice to the Commonwealth.

4. From time to time, emergency maintenance may be required to bring down the system. In such situations, if possible, the selected Offeror shall give advance notice, before the system goes down for maintenance, to the Commonwealth. The selected Offeror will limit the emergency maintenance to those situations which require immediate action of bringing down the system that cannot wait for the next scheduled maintenance period. It is expected that the Offeror will rollover to a backup site during any such emergency maintenance.

C. Security Requirements

1. The selected Offeror shall conduct a third party independent security/vulnerability assessment at its own expense on an annual basis and submit the results of such assessment to the Commonwealth within the timeframe set forth in the RFP.

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

3. The selected Offeror 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 selected Offeror shall use industry best practices to provide system intrusion detection and prevention in order to detect intrusions in a timely manner.

5. The selected Offeror shall use industry best practices to provide virus protection on all servers and network components.

6. The selected Offeror shall limit access to the system and servers and provide access only to those staff that must have access to provide services proposed.

7. The Provider will provide all Services, using security technologies and techniques in accordance with industry best practices and the Commonwealth's security policies, procedures, and requirements, including those relating to the prevention and detection of fraud and any other inappropriate use or access of systems and networks.

D. Data Storage

1. The selected Offeror shall use industry best practices to update all systems and third party software security patches to reduce security risk. The Provider shall protect their systems with 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.

2. The selected Offeror shall be solely responsible for all data storage required.

3. The selected Offeror shall take all necessary measures to protect the data including, but not limited to, the backup of the servers on a daily basis in accordance with industry best practices and encryption techniques.

4. The Provider agrees to have appropriate controls in place to protect critical or sensitive data and shall employ stringent policies, procedures, and best practices to protect that data particularly in instances where sensitive data may be stored on a Provider controlled or owned electronic device.

E. Disaster Recovery

1. The selected Offeror shall employ reasonable disaster recovery procedures to assist in preventing interruption in the use of the system.

2. The selected Offeror 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 each classification of problem.

F. Data Exchange/Interface Requirements

1. PCI Compliance (If provider processes payment card data.)

The Provider is obliged to adhere to the Payment Card Industry Data Security Standard (PCI DSS) if it processes payment card data. Moreover, The Provider certifies that their Information Technology practices conform to and meet PCI DSS standards as defined by The PCI Security Standards Council at https://www.pcisecuritystandards.org/security_standards/index.php.

The Provider will monitor these PCI DSS standards and its Information Technology practices and the Provider will notify the Commonwealth within one (1) week, if its practices should not conform to such standards. The PROVIDER will provide a letter of certification to attest to meeting this requirement and agrees to the Commonwealth's right-to-audit either by Commonwealth or external 3rd party auditors.

Provider agrees that it may (1) create, (2) receive from or on behalf of Commonwealth, or (3) have access to, payment card records or record systems containing cardholder data including credit card numbers (collectively, the "Cardholder Data"). Provider shall comply with the Payment Card Industry Data Security Standard ("PCI-DSS") requirements for Cardholder Data that are prescribed by the payment brands (as appropriate including Visa, Mastercard, American Express, Discover), as they may be amended from time to time (collectively, the "PCIDSS Requirements"). Provider acknowledges and agrees that Cardholder Data may only be used for assisting in completing a card transaction, for fraud control services, for loyalty programs, or as specifically agreed to by the payment brands, for purposes of this Agreement or as required by applicable law.

G. Adherance to Policy

1. The selected Offeror shall utilize a secured backup solution to prevent loss of data, back up all data every day and store backup media. Storage of backup media offsite is required. Stored media must be kept in an all-hazards protective storage safe at the worksite and when taken offsite. All back up data and media shall be encrypted.

2. The Provider shall abide by all the Commonwealth's policies (Information Technology Bulletins (ITBs)).

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

H. Closeout

1.. When the contract term expires or terminates, and at any other time at the written request of the disclosing Party, the receiving Party must promptly return to the disclosing Party all its Confidential Information (and all copies of this information) that is in the receiving Party's possession or control, in whatever form.