Attachment A
Requirements for Non-Commonwealth Hosted Applications/Services

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

A. Hosting Requirements

1. Licensor/Reseller shall supply all hosting equipment (hardware and software) required for performance of the software and services set forth in the Quote and Statement of Work.

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

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

4. Licensor/Reseller shall maintain all hosting equipment (hardware and software) and replace as necessary to maintain compliance with the Service Level Agreements.

5. Licensor/Reseller shall monitor, prevent and deter unauthorized system access. Any and all known attempts must be reported to the Commonwealth within **two (2)** business days or as otherwise set forth in the Software License Requirements Agreement or the Statement of Work. 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, Licensor/Reseller shall comply with state and federal data breach notification regulations and shall report security incidents to the Commonwealth within **one (1) hour** of when Licensor/Reseller has reasonable confirmation of such unauthorized access, use, release, or disclosure of data.

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

7. Licensor/Reseller staff that are directly responsible for day-to-day monitoring and maintenance shall have industry standard certifications applicable to the environment and system architecture used.

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

10. Licensor/Reseller shall completely test and apply patches for all third-party software products before release.

11. Licensor/Reseller shall provide the Commonwealth with its annual American Institute of Certified Public Accountants (AICPA) Attestation Standard (AT) Sec. 101 Service Organization Control ("SOC") 2, Type 2 certification (AT Sec. 101 SOC 2, Type 2), or an equivalent certification approved by the Commonwealth. Equivalent certifications include, but are not limited to: International Organization of Standards (ISO) 2700x certification; certification under the Federal Information Security Management Act (FISMA); and AT Sec. 101 SOC 3 (SysTrust/WebTrust) certification. Annually, Licensor/Reseller shall provide an AT Sec. 101 SOC 2, Type 2 audit report, or its equivalent, to the Commonwealth upon request.

B. System Availability (as applicable)

1. The Licensor or Reseller shall make available the system and any custom software on a *{basis for system availability ex. 24 x 7}* basis.

2. The Licensor or Reseller shall perform routine maintenance during the planned weekly maintenance period of {insert weekly maintenance period ex. Daily from Midnight to 5am Eastern time}. Routine maintenance shall include, but is not limited to, server upgrades/patching, software upgrades/patching and hardware maintenance. ***{Remove the following sentence if this is not an availability requirement}*** In order to maintain system availability, the Licensor or Reseller is expected to rollover to a backup site during maintenance periods.

3. The Licensor or Reseller shall perform non-routine maintenance at a mutually agreeable time with {insert time period for advance notice ex. 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 Licensor or Reseller shall give advance notice, before the system goes down for maintenance, to the Commonwealth. The Licensor or Reseller 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. ***{Remove the following sentence if this is not an availability requirement}*** It is expected that the will rollover to a backup site during any such emergency maintenance.

C. Security Requirements

1. Licensor/Reseller 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 {insert time period ex. three (3) business days}.

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

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

5. Licensor/Reseller shall use industry best practices to provide applicable malware and virus protection on all servers and network components.

6. Licensor/Reseller shall limit access to the Commonwealth specific systems and servers and provide access only to those staff that must have access to provide services proposed.

7. Licensor/Reseller 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 intrusions, and any other inappropriate use or access of systems and networks.

D. Data Storage

1. Licensor/Reseller shall use industry best practices to update and patch all applicable systems and third party software security configurations to reduce security risk. Licensor/Reseller 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.

2. Licensor/Reseller shall be solely responsible for applicable data storage required.

3. Licensor/Reseller shall take all commercially viable and applicable 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. Licensor/Reseller agrees to 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 sensitive data may be stored on a Licensor/Reseller controlled or owned electronic device.

5. Licensor/Reseller shall utilize a secured backup solution to prevent loss of data, back up all data every day and store backup media. Stored backup 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.

E. Disaster Recovery

Licensor/Reseller shall employ reasonable disaster recovery procedures to assist in preventing interruption in the use of the system.

Data Exchange/Interface Requirements

F. PCI Compliance {Only use if Licensor or Reseller processes payment card data.}

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

2. The Licensor or Reseller will monitor these PCI DSS standards and its Information Technology practices and the Licensor or Reseller will notify the Commonwealth within **one (1) week**, if its practices should not conform to such standards. The Licensor or Reseller 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 third party auditors.

3. Licensor/Reseller 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”). Licensor/Reseller 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”). Licensor/Reseller 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 the Agreement/Purchase Order or as required by applicable law.

G. Adherence to Policy

1. Licensor/Reseller 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.

2. Licensor/Reseller shall abide by the applicable Commonwealth's Information Technology Policies (ITPs), a list of the most relevant being attached hereto as Attachment A-1.

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

H. Closeout

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

Attachment A-1

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

ITP Number	Title	Type
ACC001	IT Accessibility Policy	Policy
APP035	Internet Browser Policy	Policy
APP036	Office Productivity Software Policy	Policy
APP037	Document Viewer and Reader Policy	Policy
INF001	Database Management Systems	Policy
INF003	Data Modeling Standards	Policy
INFRM006	Electronic Documents Management Systems	Policy
PRV001	Commonwealth of Pennsylvania Electronic Information Privacy Policy	Policy
SEC001	Enterprise Host Security Software Suite Standards and Policy	Policy
SEC004	Enterprise Web Application Firewall	Policy
SEC005	Commonwealth Application Certification and Accreditation	Policy
SEC007	Minimum Standards for User ID's and Passwords	Policy
SEC010	Virtual Private Networks	Policy

ITP Number	Title	Type
SEC011	Enterprise Policy and software Standards for Agency Firewalls	Policy
SEC019	Policy and procedures for Protecting Commonwealth Electronic Data	Policy
SEC020	Encryption Standards for Data at Rest	Policy
SEC024	IT Security Incident Reporting Policy	Policy
SEC025	Proper Use and Disclosure of Personally Identifiable Information (PII)	Policy
SEC031	Encryption Standards for Data in Transit	Policy
SEC034	Enterprise Firewall Rule Set	Policy
SYM003	Off-site Storage for Commonwealth Agencies	Policy
SYM006	Desktop and Server Software Patching Policy	Policy