# The Commonwealth of Kentucky General Provisions

## Section 1.010-Term of Contract

The initial term of Contract MA 758 2000000116-1 shall be from **October 08, 2019 thru March 9, 2024.**

## Section 1.020-Multlyear Contracts

If this Contract is for a term that extends beyond the end of the biennium in which the Contract was made, payment and performance obligations for succeeding fiscal years are subject to the availability of funds therefor. When funds are not appropriated or otherwise made available to

support continuation of performance of the Contract beyond the biennium, the Contract for such subsequent year(s) may be canceled and the Contractor shall be reimbursed in accordance with terminations provisions under 200 KAR 5:312.

## Section 1.030-Changes and Modifications to the Contract

Pursuant to KRS 45A.210(1) and 200 KAR 5:311, no modification or change of any provision in the Contract shall be made, or construed to have been made, unless such modification is mutually agreed to in writing by the Contractor and the Commonwealth, and incorporated as a written amendment to the Contract and approved by the Commonwealth prior to the effective date of such modification or change pursuant to KRS 45A.210(1) and 200 KAR 5:311. Memorandum of understanding, written clarification, and/or correspondence shall not be construed as amendments to the Contract.

If the Contractor finds at any time that existing conditions make modification of the Contract necessary, Contractor shall promptly report such matters to the Commonwealth for consideration and decision.

## Section 1.040-Payment

The Commonwealth will make payment within thirty (30) working days of receipt of Contractor's invoice, or of acceptance of goods and/or services in accordance with KRS 45.453 and KRS 45.45:4.

Payments are predicated upon successful completion and acceptance of the described work for services, and delivery of the required documentation. Invoices for payment shall be submitted to the Commonwealth.

## Section 1.050-Confidentiality of Contract Terms

The Contractor and the Commonwealth agree that all information communicated between them before the effective date of the Contract shall be received in strict confidence and shall not be disclosed by the receiving party, its agents, or employees without prior written consent of the other party. Such material will be kept confidential subject to Commonwealth and Federal public information disclosure laws.

Upon signing of the Contract by all Parties, terms of the Contract become available to the public, pursuant to the provisions of the Kentucky Revised Statutes.

The Contractor shall have an appropriate agreement with its Subcontractors who will perform under this contract, extending these confidentiality requirements to all Subcontractors' employees.

**Section 1.060-Patent or Copyright Infringement**

The Contractor shall report to the Commonwealth promptly and in reasonable written detail, each notice of claim of patent or copyright infringement based on the performance of this Contract of which the Contractor has knowledge.

The Commonwealth agrees to notify the Contractor promptly, in writing, of any such claim, suit or proceeding, and at the Contractor's expense give the Contractor proper and full information needed to settle and/or defend any such claim, suit or proceeding.

If, in the Contractor's opinion, the equipment, materials, or information mentioned in the paragraphs above is likely to or does become the subject of a claim or infringement of a United States patent or copyright, then without diminishing the Contractor's obligation to satisfy any final award, the Contractor may, with the Commonwealth's written consent, substitute other equally suitable equipment, materials, and information, or at the Contractor's options and expense, obtain the right for the Commonwealth to continue the use of such equipment, materials, and information.

The Commonwealth agrees that the Contractor has the right to defend, or at its option, to settle and the Contractor agrees to defend at its own expense, or at its option to settle, any claim, suit or proceeding brought against the Commonwealth on the issue of infringement of any United States patent or copyright or any product, or any part thereof, supplied by the Contractor to the Commonwealth under this agreement. The Contractor agrees to pay any final judgment entered against the Commonwealth on such issue in any suit or proceeding defended by the Contractor.

If principles of governmental or public law are involved, the Commonwealth may participate in the defense of any such action, but no costs or expenses shall be incurred for the account of the Contractor without the Contractor's written consent.

The Contractor shall have no liability for any infringement based upon:

- the combination of such product or part with any other product or part not furnished to the Commonwealth by the Contractor
- the modification of such product or part unless such modification was made by the Contractor
- the use of such product or part in a manner for which it was not designed

**Section 1.070-Contract Claims**

The Parties acknowledge that KRS 45A.225 to 45A.290 govern contract claims.

**Section 1.080-EEO Requirements**

The Equal Employment Opportunity Act of 1978 applies to All State government projects with an estimated value exceeding $500,000. The Contractor shall comply with all terms and conditions of the Act. A copy of the EEO forms may be obtained by downloading them from the E- **Procurement website at** http://finance.ky.gov/servlceseprocurement/Pages/VendorServices.aspx.

The Commonwealth will review the EEO Forms (or equivalent, if applicable) upon receipt. If a Vendor

is under-utilized or in non-compliance, the Vendor shall receive notification from the Commonwealth. The Vendor shall have five (5) days from receipt of such notice to submit an affirmative action plan. Failure to submit an affirmative action plan within the timeframe specified may result in the disqualification of the Vendor's response. In any event, a Vendor shall not be eligible for an award of contract without being in compliance with the EEO requirements.
If the Vendor is exempt from submitting the EEO Forms, the Vendor must state such. Exemption from EEO Form submission, under KRS 45.590, does not obviate any other requirements of KRS 45.570.

**Section 1.090-Provislons for Termination of the Contract**

This contract shall be subject to the termination provisions set forth in 200 KAR 5:312.

**Section 1.100-Conformance with Commonwealth & Federal Laws/Regulations**

This Contract is subject to the laws of the Commonwealth of Kentucky and where applicable Federal law. Any litigation with respect to this Contract shall be brought in state or federal court in **Franklin County, Kentucky.**

**Section 1.110- Commonwealth Office of Technology Requirements, if applicable**

**1. Commonwealth Information Technology Policies and Standards**
The Vendor and any subcontractors shall be required to adhere to applicable Commonwealth policies and standards, or mutually agreed upon equivalents, related to technology use and security.

**2. Compliance with Kentucky Information Technology Standards (KITS)**

A. The Kentucky Information Technology Standards (KITS) reflect a set of principles for information, technology, applications, and organization. These standards provide guidelines, policies, directional statements and sets of standards for information technology. It defines, for the Commonwealth, functional and information needs so that technology choices can be made based on business objectives and service delivery. The Vendor shall stay knowledgeable and shall abide by these standards for all related work. For example, the entire vendor solution that uses Internet Browsers as the User Interface (UI) must be fully compatible with approved browser versions listed on Kentucky Information Technology Standards (KITS) throughout the life of this project.
http://technology.ky.gov/Governance/Pages/KITS.aspx

B. The Vendor and any subcontractors shall be required to submit a technology roadmap for any offered solution. Additional roadmaps will be submitted upon request of the Commonwealth. The Roadmap shall include, but is not limited to, planned, scheduled and projected product lifecycle dates and historical release/ patch or maintenance dates for the technology. In addition, any guidance on · projected release/revision/patch/maintenance schedules would be preferred.

**3. Compliance with Commonwealth Security Standards**
The software deployment and all Vendor services shall abide by security standards as outlined in the Commonwealth's Enterprise Information Technology Policies.

**Enterprise Security Policies**
http://technology.ky.gov/ciso/Pages/lnformationSecurityPolicies,StandardsandProcedures.aspx

**Enterprise Policies**
http://technology.ky.gov/policy/pages/policies.aspx

**Finance and Administration Cabinet Commonwealth Office of Technology Enterprise IT Policies**
http://finance.ky.gov/services/policies/Pages/default.aspx

**4. Compliance with Industry Accepted Reporting Standards Based on Trust Service Principles and Criteria**

The Vendor must on an annual basis submit to DOR an AT101 SOC 2 Type II report, or equivalent, on the Controls Placed in Operation and Tests of Operating Effectiveness based upon the security requirements set forth in this section.

Further, to enhance security beyond regulatory compliance requirements, DOR combines Federal and State information security standards and requirements with industry best practices to create a comprehensive set of information security policies and standards, which are designed to support DOR's mission, vision, and organizational goals. DOR information security policies and standards may be amended from time to time as is considered necessary.

**5. System Vulnerability and Security Assessments**

The Commonwealth reserves the right to conduct external non-invasive vulnerability and security assessments of the software and infrastructure used to provide services prior to implementation and periodically thereafter. Upon completion of these assessments, the Commonwealth will communicate any findings to the Vendor for action. Any cost relating to the alleviation of the findings will be the responsibility of the Vendor. Mitigations will be subject to re-evaluation after completion. In cases where direct mitigation cannot be achieved, the Vendor shall communicate this and work closely with the Commonwealth to identify acceptable compensating controls that will reduce **risk** to an acceptable and agreed upon level. An accredited third party source may be selected by the Vendor to address findings, provided they will acknowledge all cost and provide valid documentation of mitigation strategies in an agreed upon timeframe.

**6. Privacy, Confidentiality and Ownership of Information**

The Commonwealth is the designated owner of all Commonwealth data and shall approve all access to that data. The Vendor shall not have ownership of Commonwealth data at any time. The Vendor shall be in compliance with privacy policies established by governmental agencies or by state or federal law. Privacy policy statements may be developed and amended from time to time by the Commonwealth and will be appropriately displayed on the Commonwealth portal (Ky.gov). The Vendor should provide sufficient security to protect the Commonwealth and COT data in network transit, storage, and cache. **All Commonwealth data, Including backups and archives, must be maintained at all times within the contiguous United States. All sensitive Commonwealth data, as defined** in **Enterprise Standards, must be encrypted In-transit and at rest.**

**7. Software Development**

Source code for software developed or modified by the Vendor specifically for the Commonwealth shall become property of the Commonwealth. This is not meant to include minor modifications to the Vendor software to configure the software for Commonwealth use. This is meant to include software written to add functionality to the Vendor product specifically to meet the requirements of the Commonwealth where the Commonwealth bears the entire cost of creating that functionality.

**8. License Agreements**

Software provided by the Vendor to the Commonwealth should contain a provision for perpetual licensing with all upgrade options. License agreements should also contain a provision for the

Commonwealth to maintain a version of the software in escrow in the event the Vendor is unable to continue business for financial or other business reasons.

**9. Software Version Requirements**

All commercially supported and Commonwealth approved software components such as Operating system (OS), Database software, Application software, Web Server software, Middle Tier software, and other ancillary software must be kept current. In the event that a patch interferes with the solution, the Vendor must present a plan for compliance to the Commonwealth outlining the constraints and an appropriate plan of action to bring the solution in to compliance to allow this patch to be applied in the shortest timeframe possible, not to exceed three months, unless otherwise negotiated with the Commonwealth.

The Vendors shall keep software in compliance with industry standards to support third party products such as Java, Adobe Flash, Internet Explorer, Mozilla Firefox, etc. at currently supported version, release, and patch levels, when such dependencies exist. In the event that a third party dependency interferes with the solution, the Vendor must present a plan for compliance to the Commonwealth outlining the constraints and an appropriate plan of action to bring the solution into compliance to allow this third party dependency to be updated in the
shortest timeframe possible, not to exceed three months, unless otherwise negotiated with the Commonwealth.

**10. Section 508 Compliance**

All user interfaces to the solution(s) provided, shall be warranted by the Vendor to comply with Section 508 of the Rehabilitation Act of 1973 (29 U.S.C. 794d) and the World Wide Web Consortium's (W3C) Web Content Accessibility Guidelines r,NCAG) 1.0, conformance level Double-A or greater.

**11. No Surreptitious Code Warranty**

The contractor represents and warrants that no copy of licensed Software provided to the Commonwealth contains or will contain any Self-Help Code or any Unauthorized Code as defined below. This warranty is referred to in this contract as the "No Surreptitious Code Warranty".

As used in this contract, "Self-Help Code" means any back door, time bomb, drop dead device, or other software routine designed to disable a computer program automatically with the passage of time or under the positive control of a person other than the licensee of the software. Self-Help Code does not include Software routines in a computer program, if any, designed to permit an owner of the computer program (or other person acting by authority of the owner) to obtain access to a licensee's computer system(s) (e.g. remote access) for purposes of maintenance or technical support.

As used in this contract, "Unauthorized Code" means any virus, Trojan horse, spyware, worm or other Software routines or components designed to permit unauthorized access to disable, erase, or otherwise harm software, equipment, or data; or to perform any other such actions. The term Unauthorized Code does not include Self-Help Code.

In addition, contractor will use up-to-date commercial virus detection software to detect and remove any viruses from any software prior to delivering it to the Commonwealth.
The Vendor shall defend the Commonwealth against any claim, and indemnify the Commonwealth against any loss or expense arising out of any breach of the No Surreptitious Code Warranty.

**12. Applicable Security Control Framework Compliance**

The Vendor must have an awareness and understanding of the NIST Special Publication 800- 53 Security Control Framework and employ safeguards that meet or exceed the moderate level controls as defined within the standard. These controls must provide sufficient safeguards to provide reasonable protections around the Commonwealth's data to ensure that the confidentiality, integrity, and availability are maintained at an appropriate level. These include but are not limited to:

- *Access Control*
  The Vendor must employ policy and process that provide for stringent control to limit physical and logical access to systems that house Commonwealth data to a need to know basis and provide clear separation of duties.
- *Awareness and Training*
  The Vendor must provide the appropriate role specific training for staff to ensure that there is awareness and understanding of roles and responsibilities as they relate to the protections around the Commonwealth's data.
- *Audit and Accountability*
  There must be sufficient auditing capability to ensure that actions are tracked and there is individual accountability for all actions taken by Vendor staff.
- *Configuration Management*
  The Vendor must work within established baselines that provide minimal functionality needed to ensure service delivery without exposing unnecessary risk. The Vendor must also employ structured change control processes that provide a level of coordination with the client agreed upon in a Service Level Agreement (SLA).
- *Contingency Planning*
  The Vendor must employ contingent planning policy and procedures that ensure service delivery based on agreed SLA levels while maintaining all Commonwealth data within the continental Unites States.
- *Identification and Authorization*
  The Vendor must employ appropriate identity and access management policies and procedures to ensure that access is appropriately authorized and managed at a level to ensure that access is provisioned and de-provisioned in a timely and efficient manner.
- *Incident Response*

  The Vendor must employ policy and procedures to ensure that an appropriate response to all identified security incidents are addressed in a timely manner and are reported to the appropriate parties in an agreed upon SLA timeframe. The Vendor must also ensure that all staff are sufficiently trained to ensure that they can identify situations that are classified as security incidents.
- *Maintenance*

  The Vendor must employ policy and procedures that ensure that all maintenance activities are conducted only by authorized maintenance staff leveraging only authorized maintenance tools.
- *Media Protection*

  The Vendor must employ policy and procedure to ensure that sufficient protections **exist** to protect Commonwealth data on all storage media throughout the media lifecycle and maintain documentation from media creation through destruction.
- *Physical and Environmental Controls*

  The Vendor must employ physical and environmental policies and procedures that ensure that the service and delivery infrastructure are located in a physically secure and environmentally protected environment to ensure the confidentiality, integrity, and availability of Commonwealth data.

- *Personnel Security*
  The Vendor must employ policies and procedures to ensure that all staff that have access to systems that house, transmit, or process Commonwealth data have been appropriately vetted and have been through a background check at the time _of hire and periodically thereafter.
- *System and Communications Protections*
  The Vendor must employ physical and logical protection that protect system communications and communication media from unauthorized access and ensure adequate physical protections from damage.

**Section 1.120-Purchase Order**

Any purchase order issued as a result of this contract will contain the following language pursuant to the General Services Administration's Rules for State and Local Disaster Purchasing

"This order is placed under GSA Schedule number **GS-03F-049GA** under the authority of the GSA Disaster Purchasing program. The products and services purchased will be used in preparation or response to disasters or recovery from major disaster declared by the President, or recovery from terrorism or nuclear, biological, chemical, or radiological attack."
https://www.gsa.gov/buying-selling/purchasing-prograrns/gsa-schedules/schedule-buyers/state-and-local-governments/state-and-local-disaster-purchasing