

ATTACHMENT A
CONTRACT
FOR
SCHOOL FOOD AUTHORITY POINT OF SERVICE (POS) SYSTEM

BETWEEN
THE COMMONWEALTH OF KENTUCKY
KENTUCKY DEPARTMENT OF EDUCATION

AND
HEARTLAND PAYMENT SYSTEMS LLC
dba
HEARTLAND SCHOOL SOLUTIONS

MA 758 2100000732

Gabe Hardaway, Account Specialist
217 Industrial Park Road
Harlan, KY 40831
Phone: (800) 256-8224 ext. 83961
Fax: (800) 256-8232
Garbiel.Hardaway@e-hps.com

This Master Agreement ("Contract", "Award" or "Agreement") is entered into, by and between the Commonwealth of Kentucky, Kentucky Department of Education, KDE, ("the Commonwealth" or "Customer") and Heartland Payment Systems LLC dba Heartland School Solutions, ("Contractor" or "Vendor") as the Prime Vendor.

The Commonwealth and Contractor agree to the following:

I. Scope of Contract

The Kentucky Department of Education (KDE) awards this contract to provide a comprehensive, fully integrated, operational, Point of Service (POS) system that will meet KY's School Food Authorities' (SFAs) needs over the next ten (10) years. There are approximately 195 SFAs in KY, including both public and private SFAs that will potentially utilize the POS system.

II. Negotiated Items

1. Vendor agrees to provide read access to all Kentucky SFA tickets within the vendor's ticketing system.
2. Vendor agrees to collect customer satisfaction surveys and provide the full details of all completed surveys upon request, no more than twice per year.
3. Vendor agrees to collect parent satisfaction surveys and provide the full details of all completed surveys upon request, no more than twice per year.
4. Vendor agrees to monitor system and network availability. Vendor also agrees to provide KDE with two accounts to have access to a monitoring dashboard to monitor system health.
5. Vendor agrees to the following System Availability Performance Penalties and Service Credits

| Systems Availability Performance % | Based on 240hr Month (12 hour x 5 day x 4 weeks) | Performance Penalty applies when 12 or more districts simultaneously are impacted with an outage |
|------------------------------------|--|--|
| 99.9% or above | < ~.25 hour | 0% |
| Less than 99% | > ~2 hours | 1% |
| Less than 98.5% | > ~3.5 hours | 5% |
| Less than 98% | > ~5 hours | 7% |
| 97% or less | > ~7 hours | 10% |

Based on the following:

- Production System Uptime is calculated Monday through Friday from 6:00 am Central time to 6:00 pm Central time, excluding Vendor's and SFA's standard official holidays, excluding scheduled downtime.
- Vendor will provide a minimum System Availability Performance of 99.9% per month measured. The 99.9% System Availability Performance shall not include scheduled downtime, time attributable to performance issues (including unscheduled downtime) that resulted from (i) KDE equipment and/or third-party equipment or actions, not within the sole control of Vendor and which are outside the Point of Demarcation, or (ii) the action or inaction of KDE or any individual or entity to which KDE has given access or (iii) the use of service, hardware, or software not provided by Vendor, including, but not limited to, issues resulting from inadequate bandwidth or related to third-party software or services.
- The 99.9% System Availability Performance does not apply to any performance or availability issues due to factors outside of vendor's reasonable control (for example, natural disaster, war, acts of terrorism, riots, government action, or a network or device failure external to vendor data centers including at the KDE site or between the KDE site and the Heartland data center).

Where the service credit is calculated:

- Based on 240 hour month (12 hour x 5 day x 4 weeks) and
- The performance penalty applies when 12 or more districts simultaneously are impacted with an outage.
- The calculation of the service credit percentage is based on the total annual operations maintenance cost per district/12 x number of districts impacted with an outage.
- The maximum monthly aggregate service credit in any month is 10% total of the total annual operations maintenance cost per district/12 x number of districts impacted with an outage.

6. Vendor agrees to the following Service Levels:

| Severity | Description | Response Time |
|--|---|---|
| Severity 1 <i>Critical Service Impact</i> | Issue critically affects the primary business service, major application, or mission critical system. We will work with District IT outside of business hours, as applicable, to resolve critical issues. Some examples of a Severity 1 issues are: <ul style="list-style-type: none"> • Outages (System Unavailable) (<i>Penalty Applicable-See Chart</i>) • Data integrity at risk • POS is non-operational | KDE will be notified within 1 hour of a reported incident. KDE will be notified via phone or email. |
| Severity 2 <i>Significant Service or Implementation Impact</i> | The business service, major application, or system is seriously affected or implementation stopped. No acceptable workaround is available. Some examples of Severity 2 issues are: <ul style="list-style-type: none"> • Reports give error message • Student import failed • Auditor requests | KDE will be notified within 2 hours of a reported incident. KDE will be notified via phone or email. |

7. Vendor agrees to provide KDE with a completed root cause analysis for each Severity 1 outage within 4 weeks of resolution.

8. Vendor and KDE agree to the proposed implementation rollout and estimated associated costs as detailed in Attachment Q - KDE Fee Schedule and Associated Monthly Payments. The number of SFAs and the specific SFAs selected for each phase of the rollout will jointly be determined with the vendor, KDE and the SFAs and as such the number of SFAs implemented may vary from the proposed schedule with the costs to be reduced or increased accordingly.

9. KDE agrees that the fee schedule does not include the annual maintenance fees for MCS software for Jefferson County Public Schools & Fayette County Public Schools. Vendor will continue to invoice both districts individually.

10. KDE and Vendor agree that the fee schedule does not include the Online Payment Fee Allocation (0.20% on total volume per district). The payment fee allocation will be calculated monthly, based on the July 1 - June 30 schedule, with a check to be issued to KDE by August of each cycle.

11. KDE and Vendor agree that SFAs with a current Vendor software support maintenance contract will continue to be invoiced for their current software support maintenance fees until their transition is completed.

12. Vendor agrees that any performance credit consideration during a month will be applied to that month with the invoice being reduced by the credit amount.

III. Terms and Conditions

SECTION 30 – COMMONWEALTH OFFICE OF TECHNOLOGY (COT) REQUIREMENTS

30.1 Commonwealth Information Technology Policies and Standards

- A. The vendor and any subcontractors shall be required to adhere to applicable Commonwealth policies and standards.
- B. The Commonwealth posts changes to COT Standards and Policies on its technology.ky.gov website. Vendors and subcontractors shall ensure their solution(s) comply with all posted changes. Vendors or subcontractors that cannot comply with changes shall, within thirty (30) days of the posted change, request written relief with the justification for such relief. The Commonwealth may 1) deny the request, 2) approve an exception to the policy / standard, or 3) consider scope changes to the contract to accommodate required changes. Vendors or subcontractors that do not provide the response within the thirty (30) day period shall be required to comply within ninety (90) days of the change.

30.2 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 resulting from this contract.
<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.

30.3 Compliance with Commonwealth Security Standards

The software deployment and all vendor services shall abide by privacy and security standards as outlined in the Commonwealth’s Enterprise Information Technology Policies.

Enterprise Security Policies

<http://technology.ky.gov/ciso/Pages/InformationSecurityPolicies,StandardsandProcedures.aspx>

Enterprise IT 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>

30.4 Compliance with Industry Accepted Reporting Standards Based on Trust Service Principles and Criteria

The vendor shall employ comprehensive risk and threat management controls based on defined industry standards for service organizations such as AICPA TSP section 100, Trust Services Principles and Criteria. The vendor shall annually assert compliance and engage a third party to examine such assertions and controls to provide a Report, such as AT101 SOC 2 type 2, on Controls at a Service Organization Relevant to Security, Availability, Processing Integrity, Confidentiality, and Privacy, which contains an opinion on whether the operating controls effectively support the assertions. All such reports, including publicly available reports (i.e. AT 101 SOC 3) shall be made available to the Commonwealth for review.

30.5 System Vulnerability and Security Assessments

The Commonwealth reserves the right to conduct, in collaboration with the vendor, 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.

30.6 Privacy Assessments

The Commonwealth reserves the right to conduct Privacy assessments of the collection, use, maintenance and sharing of Commonwealth data by any vendor services, software, and infrastructure used to provide services prior to implementation and periodically thereafter. Upon completion of this assessment, 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 or privacy practices 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.

30.7 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 not profit from or share Commonwealth data. The Vendor shall be in compliance with privacy policies established by governmental agencies or by state or federal law. Privacy notice 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 shall provide sufficient security to protect the Commonwealth and COT data in network transit, storage, and cache. **All Commonwealth data, including backups and archives, shall be maintained at all times within the contiguous United States. All Commonwealth data, classified as sensitive or higher, as defined in Enterprise Standards, shall be encrypted in-transit and at rest.**

30.8 **EU GDPR Compliance**

The Commonwealth of Kentucky requires all vendor contracts to comply with the European Union's General Data Privacy Regulation [Regulation (EU) 2016/679] (the "GDPR") when the Commonwealth is a "controller" or "processor" of "personal data" from an individual "data subject" located in the European Union, as those terms are defined in the GDPR. The Contractor acknowledges and agrees that it is acting as a "processor" of "personal data" for the Commonwealth under this Agreement and that all applicable requirements of the GDPR are incorporated by reference as material terms of this Agreement. The Contractor represents and warrants that (1) it is aware of and understands its compliance obligations as a "processor" under GDPR; (2) it has adopted a GDPR compliance policy/program, a copy of which has been provided to the Commonwealth; (3) it will process "personal data" only in accordance with the Commonwealth's instructions; and (4) with regard to its obligations under this Agreement, it shall comply with all applicable requirements of the GDPR to the same extent as adopted by the Commonwealth. Additionally, the Contractor shall indemnify and hold harmless the Commonwealth, and its employees from and against any claims, demands, suits, damages, penalties, fines, or costs arising from any violation of GDPR by the Contractor.

30.9 **X-as-a-Service Technical Definitions**

Refer to [NIST 800-145](#)

30.10 **Data Quality**

Vendors shall provide proposed levels of data quality per the following dimensions.

Data Quality is the degree to which data is valid, accurate, complete, unique, timely, consistent with all requirements and business rules, and relevant for a given use. The vendor shall provide data quality definitions and metrics for any data elements. Data has to be of the appropriate quality to address the needs of the Commonwealth of Kentucky. The following dimensions can be used to assess data quality:

- Validity – The data values are in an acceptable format.
- Accuracy – The data attribute is accurate.
- Completeness – There are no null values in a data field.
- Uniqueness – There are no duplicate values in a data field.
- Timeliness – The data attribute represents information that is not out-of-date.
- Consistency – The data attribute is consistent with a business rule that may be based on that attribute itself, or on multiple attributes.
- Adherence to business rules – The data attribute or a combination of data attributes adheres to specified business rules.

30.11 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.

30.12 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 shall be kept current. In the event that a patch interferes with the solution, the vendor shall present a plan for compliance with 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 dependencies such as Java, Adobe Flash, Internet Explorer, Mozilla Firefox, etc. at currently supported version, release, and patch levels. In the event that a third party dependency interferes with the solution, the vendor shall 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.

30.13 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 (WCAG) 2.0, conformance level Double-A or greater.

30.14 No Surreptitious Code Warranty

The contractor represents and warrants that no copy of licensed Software provided to the Commonwealth shall 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 shall 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.

30.15 Network Connection Requirements

A. Vendor shall work with KDE and/or all Kentucky public schools to establish any network connections. If a secure site-to-site connection is required, the vendor shall employ a secure site-to-site connection procured by KDE.

B. Vendor shall notify KDE and/or all Kentucky public schools network bandwidth requirements and if caching is required for implementation vendor shall resolve caching requirements, in coordination with KDE.

C. Vendor shall, at KDE's discretion, provide appropriate access to enable the Commonwealth to perform additional security measures, such as decryption of the network traffic if required for inspection. If the proposed solution does not have the ability to meet this requirement, the vendor shall provide an alternative such as audit reporting of this function.

D. Vendor shall provide notifications to the KDE Customer Service Center and/or applicable local school district service center for unplanned outages within 5 minutes.

E. Vendor shall notify KDE Change Management and/or applicable local school district, through the KDE Customer Service Center and/or applicable local school district, a minimum of two (2) weeks prior to any planned outage.

30.16 Application and Service Requirements

A. Current Enterprise Applications and Services

1. COT provides a number of Enterprise Shared Services to State agencies. Vendor shall use published IT Applications and Services provided on KITS for: Enterprise Service Bus, Enterprise Content Management, Data Warehousing, Data Analytics and Reporting, Business Intelligence, Web Services, GIS, unless explicitly approved by COT.

2. Vendor provided dedicated application components (i.e., Application Servers, Databases, etc.) shall comply with KITS or if the technology is not included in KITS, the technology shall be accepted by the Commonwealth for inclusion in KITS or granted a written exception to KITS according to COT Information Technology Standards Policy currently CIO-051.

3. Vendor applications shall describe in detail all available features and functionality accessible via APIs.

B. Vendor shall comply with Commonwealth of Kentucky finger print requirements for PII/FTI/HIPAA data systems hosted outside Central Data Center.

30.17 **Applicable Security Control Framework Compliance**

The vendor shall 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. The respondent must provide sufficient safeguards to provide reasonable protections around the Commonwealth's data to ensure that the confidentiality, integrity, and availability is 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, on a need to know basis, provide clear separation of duties, and adheres to least privilege principles.
- ***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 United 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 sufficient 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 to ensure adequate physical protections from damage.

SECTION 40 – PROCUREMENT REQUIREMENTS

40.1 Procurement Requirements

Procurement requirements are listed under “**Procurement Laws, Preference, Regulations and Policies**” and “**Response to Solicitation**” located on the eProcurement Web page at <https://finance.ky.gov/services/eprocurement/Pages/LawsPrefRegsPolicies.aspx> and <http://finance.ky.gov/services/eprocurement/Pages/VendorServices.aspx> respectively. The vendor must comply with all applicable statutes, regulations and policies related to this procurement.

40.2 Contract Components and Order of Precedence

The Commonwealth’s acceptance of the contractor’s offer in response to the solicitation RFP 758 2000000242, indicated by the issuance of a contract award by the Office of Procurement Services, shall create a valid contract between the Parties consisting of the following:

1. Procurement Statutes, Regulations and Policies
2. Any written Agreement between the Parties;
3. Any Addenda to the Solicitation RFP 758 2000000242;
4. The Solicitation RFP 758 2000000242 and all attachments
5. Any Best and Final Offer;
6. Any clarifications concerning the Contractor’s proposal in response to the Solicitation RFP 758 2000000242;
7. The Contractor’s proposal in response to the Solicitation RFP 758 2000000242.

In the event of any conflict between or among the provisions contained in the contract, the order of precedence shall be as enumerated above.

40.3 Final Agreement

The contract represents the entire agreement between the parties with respect to the subject matter hereof. Prior negotiations, representations, or agreements, either written or oral, between the parties hereto relating to the subject matter hereof shall be of no effect upon this contract.

40.4 Contract Provisions

If any provision of this contract (including items incorporated by reference) is declared or found to be illegal, unenforceable, or void, then both the Commonwealth and the contractor shall be relieved of all obligations arising under such provision. If the remainder of this contract is capable of performance, it shall not be affected by such declaration or finding and shall be fully performed.

40.5 Type of Contract

The contract shall be on the basis of a **firm fixed unit price** for the elements listed.

40.6 Contract Usage

As a result of this contract, the contractual agreement with the selected vendor will in no way obligate the Commonwealth of Kentucky to purchase any services or equipment under this contract. The Commonwealth agrees, in entering into any contract, to purchase only such services in such quantities as necessary to meet the actual requirements as determined by the Commonwealth.

40.7 Addition or Deletion of Items or Services

The Office of Procurement Services reserves the right to add new and similar items, by issuing a contract modification, to this contract with the consent of the vendor. Until such time as the vendor receives a modification, the vendor shall not accept delivery orders from any agency referencing such items or services.

40.8 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 processed through the Office of Procurement Services and approved by the Finance and Administration Cabinet 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 made modification of the contract necessary, it shall promptly report such matters to the Commonwealth Buyer for consideration and decision.

40.9 Changes in Scope

The Commonwealth may, at any time by written order, make changes within the general scope of the contract. No changes in scope are to be conducted except at the approval of the Commonwealth.

40.10 Contract Conformance

If the Commonwealth Buyer determines that deliverables due under the contract are not in conformance with the terms and conditions of the contract and the mutually agreed-upon project plan, the Buyer may request the contractor to deliver assurances in the form of additional contractor resources and to demonstrate that other major schedules will not be affected. The Commonwealth shall determine the quantity and quality of such additional resources and failure to comply may constitute default by the contractor.

40.11 Assignment

The contract shall not be assigned in whole or in part without the prior written consent of the Commonwealth Buyer.

40.12 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 45.454.

Payments are predicated upon successful completion and acceptance of the described work, services, supplies, or commodities, and delivery of the required documentation. Invoices for payment shall be submitted to the agency contact person or his representative.

40.13 Contractor Cooperation in Related Efforts

The Commonwealth of Kentucky may undertake or award other contracts for additional or related work, services, supplies, or commodities, and the contractor shall fully cooperate with such other contractors and Commonwealth employees. The contractor shall not commit or permit any act that will interfere with the performance of work by any other contractor or by Commonwealth employees.

40.14 Contractor Affiliation

"Affiliate" shall mean a branch, division or subsidiary that is effectively controlled by another party. If any affiliate of the contractor shall take any action that, if done by the contractor, would constitute a breach of this agreement, the same shall be deemed a breach by such party with like legal effect.

40.15 Commonwealth Property

The contractor shall be responsible for the proper custody and care of any Commonwealth-owned property furnished for contractor's use in connections with the performance of this contract. The contractor shall reimburse the Commonwealth for its loss or damage, normal wear and tear excepted.

40.16 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 necessarily 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 extending these confidentiality requirements to all subcontractors' employees.

40.17 Confidential Information

The contractor shall comply with the provisions of the Privacy Act of 1974 and instruct its employees to use the same degree of care as it uses with its own data to keep confidential information concerning client data, the business of the Commonwealth, its financial affairs, its relations with its citizens and its employees, as well as any other information which may be specifically classified as confidential by the Commonwealth in writing to the contractor. All

Federal and State Regulations and Statutes related to confidentiality shall be applicable to the contractor. The contractor shall have an appropriate agreement with its employees, and any subcontractor employees, to that effect, provided however, that the foregoing will not apply to:

- A. Information which the Commonwealth has released in writing from being maintained in confidence;
- B. Information which at the time of disclosure is in the public domain by having been printed or published and available to the public in libraries or other public places where such data is usually collected; or
- C. Information, which, after disclosure, becomes part of the public domain as defined above, through no act of the contractor.

40.18 Advertising Award

The contractor shall not refer to the award of contract in commercial advertising in such a manner as to state or imply that the firm or its services are endorsed or preferred by the Commonwealth of Kentucky without the expressed written consent of the agency technical contact person. (see Section 50.4)

40.19 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 option 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:

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

40.20 Permits, Licenses, Taxes and Commonwealth Registration

The contractor shall procure all necessary permits and licenses and abide by all applicable laws, regulations, and ordinances of all Federal, State, and local governments in which work under this contract is performed.

The contractor shall maintain certification of authority to conduct business in the Commonwealth of Kentucky during the term of this contract. Such registration is obtained from the Secretary of State, who will also provide the certification thereof. Additional local registration or license may be required.

The contractor shall pay any sales, use, and personal property taxes arising out of this contract and the transaction contemplated hereby. Any other taxes levied upon this contract, the transaction, or the equipment or services delivered pursuant hereto shall be borne by the contractor.

40.21 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.

<http://finance.ky.gov/services/eprocurement/Pages/VendorServices.aspx>.

40.22 Provisions for Termination of the Contract

Any contract resulting from this contract shall be subject to the termination provisions set forth in 200 KAR 5:312.

40.23 Bankruptcy

In the event the contractor becomes the subject debtor in a case pending under the Federal Bankruptcy Code, the Commonwealth's right to terminate this contract may be subject to the rights of a trustee in bankruptcy to assume or assign this contract. The trustee shall not have the right to assume or assign this contract unless the trustee (a) promptly cures all defaults under this contract; (b) promptly compensates the Commonwealth for the monetary damages incurred as a result of such default, and (c) provides adequate assurance of future performance, as determined by the Commonwealth.

40.24 Conformance with Commonwealth & Federal Laws/Regulations

This contract shall be governed by and construed in accordance with the laws of the Commonwealth of Kentucky. Any action brought against the Commonwealth on the contract, including but not limited to actions either for breach of contract or for

enforcement of the contract, shall be brought in Franklin Circuit Court, Franklin County, Kentucky in accordance with KRS 45A.245.

40.25 Accessibility

Vendor hereby warrants that the products or services to be provided under this contract comply with the accessibility requirements of Section 504 of the Rehabilitation Act of 1973, as amended (29 U.S.C. § 794d), and its implementing regulations set forth at Title 36, Code of Federal Regulations, part 1194. Vendor further warrants that the products or services to be provided under this contract comply with existing federal standards established under Section 255 of the Federal Telecommunications Act of 1996 (47 U.S.C. § 255), and its implementing regulations set forth at Title 36, Code of Federal Regulations, part 1193, to the extent the vendor's products or services may be covered by that act. Vendor agrees to promptly respond to and resolve any complaint regarding accessibility of its products or services which is brought to its attention.

40.26 Access to Records

The state agency certifies that it is in compliance with the provisions of KRS 45A.695, "Access to contractor's books, documents, papers, records, or other evidence directly pertinent to the contract." The Contractor, as defined in KRS 45A.030, agrees that the contracting agency, the Finance and Administration Cabinet, the Auditor of Public Accounts, and the Legislative Research Commission, or their duly authorized representatives, shall have access to any books, documents, papers, records, or other evidence, which are directly pertinent to this agreement for the purpose of financial audit or program review. The Contractor also recognizes that any books, documents, papers, records, or other evidence, received during a financial audit or program review shall be subject to the Kentucky Open Records Act, KRS 61.870 to 61.884. Records and other prequalification information confidentially disclosed as part of the bid process shall not be deemed as directly pertinent to the agreement and shall be exempt from disclosure as provided in KRS 61.878(1)(c).

40.27 Prohibitions of Certain Conflicts of Interest

In accordance with KRS 45A.340, the contractor represents and warrants, and the Commonwealth relies upon such representation and warranty, that it presently has no interest and shall not acquire any interest, direct or indirect, which would conflict in any manner or degree with the performance of its services. The contractor further represents and warrants that in the performance of the contract, no person, including any subcontractor, having any such interest shall be employed.

In accordance with KRS 45A.340 and KRS 11A.040 (4), the contractor agrees that it shall not knowingly allow any official or employee of the Commonwealth who exercises any function or responsibility in the review or approval of the undertaking or carrying out of this contract to voluntarily acquire any ownership interest, direct or indirect, in the contract prior to the completion of the contract.

40.28 No Contingent Fees

No person or selling agency shall be employed or retained or given anything of monetary value to solicit or secure this contract, excepting bona fide employees of the offeror or bona fide established commercial or selling agencies maintained by the offeror for the purpose of

securing business. For breach or violation of this provision, the Commonwealth shall have the right to reject the proposal or cancel the contract without liability.

40.29 Intentionally Omitted

40.30 Contract Claims

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

40.31 Limitation of Liability

The liability of the Commonwealth related to contractual damages is set forth in KRS 45A.245.

40.32 Discrimination (Effective April 8, 2015)

Discrimination (because of race, religion, color, national origin, sex, sexual orientation, gender identity, age, or disability) is prohibited. This section applies only to contracts utilizing federal funds, in whole or in part. During the performance of this contract, the contractor agrees as follows:

1. The contractor will not discriminate against any employee or applicant for employment because of race, religion, color, national origin, sex, sexual orientation, gender identity, or age. The contractor further agrees to comply with the provisions of the Americans with Disabilities Act (ADA), Public Law 101-336, and applicable federal regulations relating thereto prohibiting discrimination against otherwise qualified disabled individuals under any program or activity. The contractor agrees to provide, upon request, needed reasonable accommodations. The contractor will take affirmative action to ensure that applicants are employed and that employees are treated during employment without regard to their race, religion, color, national origin, sex, sexual orientation, gender identity, age or disability. Such action shall include, but not be limited to the following; employment, upgrading, demotion or transfer; recruitment or recruitment advertising; layoff or termination; rates of pay or other forms of compensations; and selection for training, including apprenticeship. The contractor agrees to post in conspicuous places, available to employees and applicants for employment, notices setting forth the provisions of this non-discrimination clause.
2. The contractor will, in all solicitations or advertisements for employees placed by or on behalf of the contractor, state that all qualified applicants will receive consideration for employment without regard to race, religion, color, national origin, sex, sexual orientation, gender identity, age or disability.
3. The contractor will send to each labor union or representative of workers with which he has a collective bargaining agreement or other contract or understanding, a notice advising the said labor union or workers' representative of the contractor's commitments under this section, and shall post copies of the notice in conspicuous places available to employees and applicants for employment. The contractor will take such action with respect to any subcontract or purchase order as the administering agency may direct as a means of enforcing such provisions, including sanctions for noncompliance.
4. The contractor will comply with all provisions of Executive Order No. 11246 of September 24, 1965 as amended, and of the rules, regulations and relevant orders of the Secretary of Labor.
5. The contractor will furnish all information and reports required by Executive Order No. 11246 of September 24, 1965, as amended, and by the rules, regulations and orders of the

Secretary of Labor, or pursuant thereto, and will permit access to his books, records and accounts by the administering agency and the Secretary of Labor for purposes of investigation to ascertain compliance with such rules, regulations and orders.

6. In the event of the contractor's noncompliance with the nondiscrimination clauses of this contract or with any of the said rules, regulations or orders, this contract may be cancelled, terminated or suspended in whole or in part and the contractor may be declared ineligible for further government contracts or federally-assisted construction contracts in accordance with procedures authorized in Executive Order No. 11246 of September 24, 1965, as amended, and such other sanctions may be imposed and remedies invoked as provided in or as otherwise provided by law.
7. The contractor will include the provisions of paragraphs (1) through (7) of section 202 of Executive Order 11246 in every subcontract or purchase order unless exempted by rules, regulations or orders of the Secretary of Labor, issued pursuant to section 204 of Executive Order No. 11246 of September 24, 1965, as amended, so that such provisions will be binding upon each subcontractor or vendor. The contractor will take such action with respect to any subcontract or purchase order as the administering agency may direct as a means of enforcing such provisions including sanctions for noncompliance; provided, however, that in the event a contractor becomes involved in, or is threatened with, litigation with a subcontractor or vendor as a result of such direction by the agency, the contractor may request the United States to enter into such litigation to protect the interests of the United States.

SECTION 50 – SCOPE OF WORK

50.1 Agencies to Be Served

This contract shall be for use by KY public school districts, the KY School for the Blind (KSB), the KY School for the Deaf (KSD), and the KY Education and Workforce Development Cabinet which includes but is not limited to the KY Department of Education (KDE), the Education Professional Standards Board (EPSB), KY Educational Television (KET) and the Council on Postsecondary Education (CPE). No shipments shall be made except upon receipt by Vendor of an official Delivery Order from a using agency.

50.2 Term of Contract and Renewal Options

The initial term of the contract shall be for a period of **five (5) years** from the effective date of the Award of Contract.

This contract may be renewed at the completion of the initial contract period for **five (5) additional one-year** periods upon the mutual agreement of the Parties. Such mutual agreement shall take the form of a contract modification as described in Section 40.8 of this contract.

At the end of the contract, the vendor shall provide all agency data in a form that can be converted to any subsequent system of the agency's choice. The vendor shall cooperate to this end with the vendor of the agency's choice, in a timely and efficient manner.

The Commonwealth reserves the right not to exercise any or all renewal options. The Commonwealth reserves the right to extend the contract for a period less than the length of the

above-referenced renewal period if such an extension is determined by the Commonwealth Buyer to be in the best interest of the Commonwealth.

The Commonwealth reserves the right to renegotiate any terms and/or conditions as may be necessary to meet requirements for the extended period. In the event proposed revisions cannot be agreed upon, either party shall have the right to withdraw without prejudice from either exercising the option or continuing the contract in an extended period.

50.3 Basis of Price Revisions

PRICE ADJUSTMENTS: Unless otherwise specified, the prices established by the contract shall remain firm for the contract period subject to the following:

- A. **Price Increases:** A price increase shall not occur during the first twelve (12) months of the contract. A vendor may request a price increase after twelve (12) months of the contract, which may be granted or denied by the Commonwealth. Any such price increase shall be based on industry wide price changes. The contract holder must request in writing a price increase at least thirty (30) days prior to the effective date, and shall provide firm proof that the price increase(s) is justified. The Office of Procurement Services may request additional information or justification. If the price increase is denied, the contract holder may withdraw from the contract without prejudice upon written notice and approval by the Office of Procurement Services. Provided, however, that the vendor must continue service, at the contract prices, until a new contract can be established (usually within sixty (60) days).
- B. **Price Decreases:** The contract price shall be reduced to reflect any industry wide price decreases. The contract holder is required to furnish the Office of Procurement Services with notice of any price decreases as soon as such decreases are available.
- C. **Extended Contract Periods:** If the contract provides for an optional renewal period, a price adjustment may be granted at the time the contract is renewed, subject to price increase justification as required in Paragraph A "Price Increases" as stated above.

50.4 Notices

After the award of contract, all programmatic communications with regard to day-to-day performance under the contract are to be made to the agency technical contact.

Kentucky Department of Education Technical Contact:

Tim Cooper

Division of School and Community Nutrition

Office of Finance and Operations

Kentucky Department of Education

300 Sower Blvd, 5th Floor

Frankfort, KY 40601

502-564-5625 x4935

Timothy.Cooper@education.ky.gov

After the award of contract, all communications of a contractual or legal nature are to be made to the Commonwealth Buyer.

Commonwealth Buyer:
Stacy Blank, CPPO
IT Division Director
COMMONWEALTH OF KENTUCKY
FINANCE AND ADMINISTRATION CABINET
Office of Procurement Services
New Capitol Annex
702 CAPITOL AVE RM 096
FRANKFORT, KY 40601
(502) 564-2294
Stacy.Blank@ky.gov

50.5 Subcontractors

The contractor is permitted to make subcontract(s) with any other party for furnishing any of the work or services herein. The contractor shall be solely responsible for performance of the entire contract whether or not subcontractors are used. The Commonwealth shall not be involved in the relationship between the prime contractor and the subcontractor. Any issues that arise as a result of this relationship shall be resolved by the prime contractor. All references to the contractor shall be construed to encompass both the contractor and any subcontractors of the contractor.

50.6 Scope of Work/Technical Requirements

A. Training and Support and Status

1. Vendor shall provide current user documentation for every module for all user types. Documentation should be easily accessible and navigable electronically by all users via direct links that are contextual within the system.
2. Vendor shall provide a single toll-free phone number for support calls that is staffed from 7:00 AM ET to 6:00 PM ET Monday – Friday excluding the following holidays: Martin Luther King Day, Memorial Day, Independence Day, Labor Day, Thanksgiving, Christmas Eve, Christmas Day, New Years' Eve and New Years' Day.
3. Vendor shall not charge for additional support functions including data corrections or required functions such as roll-over as users should be trained and solution should provide necessary functionality.
4. Vendor shall change the 'out-of-the-box' Administrator username and password across their machines at implementation.
5. Vendor should provide a documented escalation path for how reported issues will be triaged, assigned, tracked and communicated to customs with associated escalation timeframes.
6. Vendor should provide a root cause analysis for all critical system outages within five (5) business days of outage resolution where an outage is defined as any critical component being unavailable for 30 minutes or more.
7. Vendor should track all user support calls by support type needed (such as by module and screen) and provide the data to KDE by the 15th of each month. Reports should include data such as district, case #, source of contact (e.g. email, phone, etc.) date responded, date resolved, resolution provided, etc.

8. Vendor should provide incremental upgrades and enhancements following a published product roadmap that is created in conjunction with KDE feedback.
9. Vendor should propose a solution to provide a running monthly summary of the following to KDE within five (5) business days after the last day of each month:
 - Average Daily Participation (ADP) by meal type by site/school by SFA.
 - Total funds added via online payment and total fees charged for online payments by site/school by SFA.
 - Total number of enrolled students by site/school by SFA
 - Total number of students by eligibility type by site/school by SFA.
 - Total number of POS terminals by site/school by SFA.
10. During an outage, the vendor should provide hourly status updates until a resolution is reached if requested by KDE. An outage is defined as any critical component being unavailable for 30 minutes or more.
11. Vendor should provide video instructions for online learning/training opportunities for all primary system functions.
12. Vendor should provide onsite training and technical assistance prior to and during system implementation period. Costs associated with training and technical assistance should be included in the vendor's component cost response.
13. Vendor should offer support help cases via multiple sources such as email, chat and phone call.
14. Vendor should provide the same level of support to all users. Vendor should provide technical support with skilled support staff who can resolve majority of reported problems via phone support or remote access.
15. Vendor should establish a consistent maintenance window outside of normal business hours for standard system maintenance outages to limit user impact.

B. Environment

1. Solution shall be offered as a cloud-based vendor hosted service managed by the vendor.
2. Solution shall be secured keeping up with current Transport Layer Security (TLS) standards.
3. Solution shall be easily scalable for adding all SFAs, sites/schools, serving lines and users.
4. System shall be fully accessible via standard internet browsers, including, at a minimum, Internet Explorer/Edge, Chrome, Safari, and Firefox and vendor shall promptly respond to and resolve any complaint regarding accessibility of its products or services which is brought to its attention.
5. System 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 (WCAG) 2.0, conformance levels A and AA or greater.
6. Solution shall allow for SFAs to purchase all necessary hardware from other sources including peripheral devices (excluding application scanners). Vendor shall provide the minimum and recommended technical specifications of all related hardware.
7. Solution shall include an audit trail to track all transactions and actions with the username, time and date of transactions via user interface.

8. Solution shall meet all data security and data breach protocols as outlined in Attachment C - Security and Data Breach Protocols.
9. Solution shall offer customized security groups within the solution allowing/disallowing users, the ability to add/edit/delete students, add/edit login accounts, run specific modules, assign eligibility, print reports, adjust account balances, etc.
10. Solution shall be able to handle high load times (such as beginning of school year application processing period) with no decrease in performance.
11. The solution shall offer federation to Microsoft Azure Active Directory, enabling Single Sign-On, describe the approach.
12. Solution should have federation to G Suite, describe the approach.
13. Solution should allow for configuration of strong passwords, allow the user to change or reset their own password and should include the following: 1) use encrypted connections whenever a password is requested, 2) store only a salted hash value for each password, 3) salt passwords with a minimum of 32 bits of data, 4) allow at least 64 characters in passwords, 5) allow any character including Unicode, 6) allow SFA to force password composition and expiration rules, and 7) allow paste into password fields.
14. Solution should provide a test environment for user testing and approval of all system changes prior to implementation in the production environment
15. Solution shall be and remain the same product and version for all SFAs.
16. Solution should provide access to past (five) 5 years' data. Access should be available via similar navigation as current navigation.
17. Solution should have the ability to daily back-up, archive and restore data in its entirety and by site/school and by module.
18. Solution should be able to handle the capacity of the largest KY SFAs (see Attachment D - 2018-2019 Qualifying Data). Solution should offer periodic software updates and improvements along with updated instructions as part of the annual maintenance plan (no additional cost) that limits the impact on users during peak usage times.
19. Solution should be on a single web-based platform not requiring multiple logins or tabs or browsers.
20. Solution should be designed to operate with standard internet browsers including at a minimum Chrome, Edge, Safari and Firefox. Solution should support new, stable browser versions within 6 months of their release and should at all times support usage of all stable versions released within the prior year. Solution should not rely on unusual or customized browser or network configuration requirements.
21. Solution should provide a training environment.

C. Point of Service

1. Solution shall require individual login/logoff with individual cashier user passwords.
2. Solution shall provide a single key for meal combinations for all meal types.
3. Solution shall display amount tendered and change due from cashier.
4. Solution shall allow for cash or check payments and for tracking of check numbers from the point service or back office.
5. Solution shall support touch screen monitors at the cashier station as well as non-touch screen setup.
6. Solution shall allow cashier to search by account name, student ID, PIN and homeroom/first period.

7. Solution shall provide the ability to store and display photos for all accounts. Solution shall allow for bulk uploading of photos. Solution should provide the ability to capture pictures at the POS.
8. Solution shall prevent overt identification keeping student eligibility status confidential during transactions.
9. Solution shall allow for students to be identified at the POS terminal in multiple ways, including at least the following methods: cashier entry, student PIN number, ID card swipe/barcode scan.
10. Solution shall allow for queuing of accounts by PIN pad entry to speed up service at Point of Service.
11. Solution shall provide the ability to customize all POS terminal screen layouts from a central login.
12. Solution shall remain functional if network connectivity is lost. Solution should provide the terminal user an on-screen notice of the loss of connectivity and shall sync the data when connection is restored without user intervention.
13. Solution shall support many serving lines within a single school including mobile point of sales.
14. Solution shall support all child nutrition programs allowable by SFAs (<https://www.fns.usda.gov/programs>).
15. Solution shall allow multiple meal prices at one school.
16. Solution shall allow for bulk entry of meal counts.
17. Solution shall provide the ability to create notes and alerts to be associated with accounts that are automatically displayed to the cashier where alerts must be acknowledged before recording the transaction.
18. Solution shall sync daily meals served by category, revenues by meal type and a la carte sales.
19. Solution shall include sync processes that do not require user initiation and do not interrupt or slow down transactions.
20. Solution shall update near real-time with student eligibility information (where near real-time is considered within three (3) seconds of submission).
21. Solution shall update near real-time with account balance changes from online payment system.
22. Solution shall track reimbursable and non-reimbursable meals.
23. Solution should provide central office view of the status of all terminals.
24. Solution should not allow for non-active accounts to be used.
25. Solution should be user friendly and easy for a novice to use with all primary functions reachable in three clicks or less. A novice would be a user who has basic familiarity with Microsoft Windows and knows how to open and use a web browser.
26. Solution should display human readable warning or error messages whenever appropriate to include suspicious transaction alert mechanism when an unusual event occurs.
27. Solution should alert cashier when a student account is accessed twice during the same meal period. Solution should include user options for second meal pricing.
28. Solution should display account balance and provide warning message where warning message threshold is defined by SFA by account type by site/school.
29. Solution should allow for an efficient lookup and use of accounts across the SFA from any site within the SFA.

30. Solution should provide a method for managers to correct/change transactions and should provide the ability to document the reasons for the changes.
31. Solution should allow a la carte and adult meals to be blocked from account charging by site/school/account.
32. Solution should allow for setting account charge limits by site/school and by account type and by specific account. Solution should allow for recording an alternate meal for students who have exceeded the charge limit.
33. Solution should allow for selecting individual food items and the system determine if it is a completed reimbursable meal.

D. Enrollment

1. Solution shall provide near real-time unattended syncing of enrollment records (enrollments, withdraws, etc.) with the state student information system.
2. Solution shall provide near real-time unattended syncing of households as defined in the state student information system.
3. Solution shall allow for manually creating enrollment records and should default the city, state, area code and any other possible fields.
4. Solution shall provide an audit trail of households when there is impact on eligibility status.
5. Solution shall maintain an audit check to prevent duplicate transfer of data and a means for alerting on failed or incomplete transfer/syncing.
6. Solution shall allow for automatically assigning unique PIN numbers for each account in an SFA and shall allow for manually changing the pin number.
7. Solution shall retain the PIN number assignments throughout a student's time enrolled in the SFA.
8. Solution should allow for multiple student information system schools to be configured to sync to one POS site.
9. Solution should include a process for looking up and transferring of student eligibility records from one SFA to another. The eligibility status that is transferred should include supporting data such as how the eligibility was determined (such as income application, direct certification, or direct certification extension), determining official, determination date, etc.
10. Solution should offer the ability for SFAs to add additional custom fields within student enrollment records to track locally defined data.
11. Solution should share with KDE unabridged results of annual audit, such as SSAE16 SOC Type 2, in addition to allowing KDE to investigate any records or other data related to findings that affect KDE or KY school districts.

E. Application Management and Eligibility Processing

1. Solution shall provide integrated online applications for parents to include both National School Lunch Applications and KY Household Income Form application as determined by the school type (CEP school = National School Lunch Application, Non-CEP school = KY Household Income Form).
2. Solution shall use a unique meal application number to track a household and that number should not be re-used.
3. Solution shall provide application management functions for processors, school sites and management and include the ability to process all types of individual and family

- applications (Income, SNAP/TANF, Foster, Homeless, Runaway, Migrant, Incomplete and Parent Refused Benefits.)
4. Solution shall recognize duplicate applications and prompt the user before processing.
 5. Solution shall include automatic updates regarding Free and Reduced income limits, as established each year by the USDA.
 6. Solution shall track history for incomplete or denied applications, including reasons application is incomplete or denied as displayable content.
 7. Solution shall offer the ability to process scanned applications.
 8. Solution shall have the capability to produce multiple types of notification letters and e-mails including but not limited to approval, denial, incomplete application and verification status/results with customization of letter content through data stored within the application. Letters and emails should be available in multiple languages to include English and Spanish at a minimum.
 9. Solution shall provide the ability for verification processing.
 10. Solution shall provide export or sync of required student Free and Reduced-Price eligibility information to the student information system.
 11. Solution shall carryover student status at the beginning of the year from the previous year during carryover period.
 12. Solution shall allow students who transfer from a Community Eligibility Provision (CEP) school to a non-CEP school 30 days of free eligibility status or until changed.
 13. Solution should have the ability to produce a student eligibility upload file to be used for Administrative Reviews. Current requirements are attached as Attachment G - Student Eligibility Upload.
 14. Solution should provide an instant analysis of Free and Reduced meal applications for eligibility according to current federal guidelines and display results on a status screen.
 15. Solution should allow for adding internal use only notes and file attachments to track related communications.
 16. Solution should have the capability to automatically deny eligibility for any applications selected for verification that do not provide a response after a specific period of time.
 17. Solution should provide online applications in multiple languages to include English and Spanish at a minimum.
 18. Solution should provide easy to follow instructions and process to aid families in completing the applications both on a computer as well as mobile device. Solution shall provide the use of back and next buttons without losing information.

F. Online Parent/Guardian Payment System

1. Solution shall allow for adding funds to student accounts via a secure web-based interface.
2. Solution shall allow free and secure web-based access to parents/guardians with the vendor providing support via a toll-free phone number and email. Solution shall be secured keeping up with current TLS standards
3. Solution shall not share or store credit card information with third parties other than the card brands and merchant banks. Credit card interface shall be PCI compliant.
4. Solution shall allow for direct payment transfers to the SFA bank account daily.
5. Solution shall settle funds directly to the SFA's designated bank account.
6. Solution shall propose a fee structure to be charged to the parent/guardian for utilizing the online payment system to cover transaction costs and revenue with a defined

portion of the revenue being given to KDE on a monthly basis along with detailed accounting of the revenue stream.

7. Solution shall seamlessly integrate with the point of service to automatically update account balance.
8. Solution should provide parents/guardians access to payment history and meal details history including a la carte purchases.
9. Solution should allow for parents/guardians to elect to receive low account balance notifications via email and sms.
10. Solution should allow for parents/guardians to elect to receive menu change notifications via email and sms.

G. Direct Certification

1. Solution shall provide an automated solution for storing direct certification records provided by the state (provided as an automated monthly dataset each month of all KY children who are currently receiving SNAP, TANF/KTAP, Medicaid or who are in Foster Care. (See Attachment E - Direct Certification Data.).
2. Solution shall include a proposal for how to best match enrollment records with direct certification records. Matching solution should include levels of confidence with configuration options for what level of confidence creates automatic record updates.
3. Solution shall allow for automated updating a student's meal status if they are directly certified with a high confidence level match. Solution shall automatically extend categorical eligibility where allowed.
4. Solution shall include a means for displaying the history of matches and associated household extensions and automatically update household member meal statuses accordingly.
5. Solution shall assign and update matched direct certification records by proper priority order.
6. Solution shall include a proposal for providing an unmatched student list work queue for manual matching sorted by match probabilities.
7. Solution should automatically attempt to match all previously unmatched records when a new monthly dataset is provided.
8. Solution should automatically attempt to match all new enrollment records.

H. Reporting and Claim Management

1. The solution shall produce all state and federally required reports.
2. The solution shall be updated to satisfy any new or updated required state or federal reporting requirements within 9 months of notice of the changes.
3. The solution shall produce a monthly site claim file for all sites that will allow for import of claim numbers to the state child nutrition information and payment solution (CNIPS). Current requirements are attached (See Attachment F - CNIPS SNP Point of Sale (POS) File Format Specifications).
4. Solution shall provide the ability to produce point in time reports. For example, a report listing student eligibilities as of April 1st shall show the same results if it is run on April 1st or any other date post April 1st regardless of program year.
5. Solution should provide all reports in multiple output options. At a minimum, all data reports shall be exportable to csv and pdf.

6. The solution should produce a detailed listing supporting any aggregate number included on a state or federally required report.
7. Solution should enable food service office staff users to build reports and select desired fields and placement of fields, add automatic calculations and summary data, store as a saved report template, and share stored template reports with other users.
8. Solution should provide onscreen viewing prior to printing reports.
9. Solution should provide reports in a consistent style including layout and consistent use of fonts and font sizes wherever practical.

I. Overall Solution

1. Solution shall comply with current state and federal laws, policies and regulations, including, but not limited to, those related to the United States Department of Agriculture (USDA). Solution shall also comply with the Family Education Rights and Privacy Act (FERPA) at 20 U.S.C. § 1232g and 34 CFR Part 99 and the KY Family Educational Rights and Privacy Act at KRS 160.700 et. seq. Solution shall maintain the security of PII and PCI data, and the vendor shall remain cognizant of, and obey, federal and state data privacy, security and breach notification laws and regulations.
2. Solution shall remain in compliance with future state and federal laws, policies and regulations.
3. Solution shall allow state users account authentication to have view access to all SFA systems.
4. Vendor should offer additional modules for purchase by SFA such as Inventory Management, Menu Planning and Production Records, Order Management, etc.
5. Solution should allow for individual SFA branding where possible (such as page headers and footers).
6. Solution should incorporate national interoperability standards (e.g., Ed-Fi, One Roster, TLS, API) vs proprietary solutions when applicable standard solutions exist.

J. Uniform Administrative Requirements, Cost Principles and Audit Requirements

1. Vendors providing service under this contract shall conform and otherwise comply with all Uniform Administrative Requirements, Cost Principles and Audit Requirements for Federal Awards as applicable. Requirements are located on the Code of Federal Regulations web page at <https://www.ecfr.gov/cgi-bin/retrieveECFR?gp=&SID=366afee6cb0855060cf7f2c5d3eae3e7&mc=true&n=pt2.1.200&r=PART&ty=HTML>

K. Value-Added Services

Value-added services may be added to the contract with prior approval by the Commonwealth Office of Technology and the Office of Procurement Services Buyer of Record. Upon approval, a formal modification will be made to add the service(s). No work shall begin until a contract modification is completed and notice provided by the OPS Buyer that work may begin.

IV. Pricing

| | |
|---|-------------------|
| Implementation Cost per SFA | \$0.00 |
| Annual Operations/Maintenance Costs per SFA | \$3,995.00 |
| Online Payment Fee Allocation % to State per SFA | 0.20% |

V. Approvals

This Contract is subject to the terms and conditions as stated. By executing this Contract, the parties verify that they are authorized to bind this agreement and that they accept the terms of this agreement.

This Contract may be executed electronically in any number of counterparts, each of which shall be deemed to be an original, but all of which together shall constitute one and the same Contract.

This Contract is invalid until properly approved and executed by the Finance and Administration Cabinet.

1st Party: Kentucky Department of Education (KDE), ("the Commonwealth" or "Customer")

Karen Wirth

Printed name
DocuSigned by:
Karen Wirth

Signature

Director

Title
3/26/2021

Date

2nd Party: Heartland Payment Systems LLC dba Heartland School Solutions, as Contracting Agent ("Contractor" or "Vendor")

Jeremy Loch

Printed name
Jeremy Loch

Signature

SVP & General Manager, School Solutions

Title
3/17/21

Date

**Approved by the Finance and Administration Cabinet
Office of Procurement Services**

Joan Graham

Printed name
DocuSigned by:
Joan Graham

Signature

Executive Director

Title
3/29/2021

Date

ATTACHMENTS:

- ATTACHMENT A – This Document**
- ATTACHMENT B – Intentionally Omitted**
- ATTACHMENT C – Intentionally Omitted**
- ATTACHMENT D – Intentionally Omitted**
- ATTACHMENT E – The Protection of Personal Information Security and Breach Investigation Procedures and Practice Act (KRS 61.931)**
- ATTACHMENT F – Intentionally Omitted**
- ATTACHMENT G – Security and Data Breach Protocols**
- ATTACHMENT H – 2018-2019 Qualifying Data**
- ATTACHMENT I – Direct Certification Data**
- ATTACHMENT J – CNIPS SNP Point of Sale (POS) File Format Specifications**
- ATTACHMENT K – Student Eligibility Upload**
- ATTACHMENT L – Mandatory Requirements - Completed**
- ATTACHMENT M – Intentionally Omitted**
- ATTACHMENT N – Intentionally Omitted**
- ATTACHMENT O – Intentionally Omitted**
- ATTACHMENT P – Intentionally Omitted**
- ATTACHMENT Q – KDE Fee Schedule and Associated Monthly Payments**