OFFICE OF COUNTY MAYOR GLENN JACOBS

Procurement Division, 1000 N. Central Street, Suite 100, Knoxville, TN 37917

KNOX COUNTY GOVERNMENT
PROCUREMENT DIVISION
ADDENDUM II TO REQUEST FOR PROPOSAL 3454
EMERGENCY MEDICAL SERVICES

ADDENDUM DATE: **September 1, 2023**

BUYER: **Jay Garrison, CPPO, CPPB**

ORIGINAL CLOSING DATE: **September 12, 2023, at 2:00 PM, local time**

The following is for clarification.

Question 1. **Section 2.22 – TERMINATION**

Question: Will there be any mechanism in the contract for the Contractor to recoup a portion of its significant initial capital expenditures to become operational if the County terminates the agreement without cause early in the term?

Answer 1. No, but could have the option to purchase at Fair Market Value.

Question 2. **Section 3.15 - EXCEPTIONS TO SPECIFICATIONS:** Vendors taking exception to any part or section of these specifications shall indicate such exceptions on their submittal. A failure to indicate any exception(s) shall be interpreted as the Vendor's intent to fully comply with the specifications as written. Conditional or qualified offers are subject to rejection in whole or in part. Any exceptions shall be included in Tab VI of the submittal. Do not strike through or in any other way alter the RFP. Exceptions listed within other sections of the submittal shall not be reviewed or considered.

Question: Does this mean that if a vendor takes exception to any section of the RFP, with the exception of Tab VI, the vendor's proposal is rejected?

Answer 2. Proposers are allowed to take exception to any sections of this RFP (excluding Section II, Obligations, Rights and Remedies) without being disqualified from consideration for award. Section II shows the requirements of the County as set forth in federal, state and/or local laws, ordinances, statutes, policies, etc. If any exceptions are taken to Section II, this may be Just Cause to deem a proposal as non-responsive and disqualified for consideration for award.

Question 3. **Section 3.20 - MINIMUM QUALIFICATION EXPECTATIONS:** Respondent must address all submittal requirements as defined in Section V, Clinical Standards. Respondent shall have a minimum of three (3) years of experience and sufficient capabilities and resources to carry out the work contemplated, as well as the equipment and personnel available for the work.

Question: How can the vendor meet the equipment and personnel "available for the work" requirement before the vendor is awarded the contract and authorized to start up services?

Answer 3 Knox County's expectation is the awarded vendor will be available for work on the contract start date of February 1, 2024.

Question 4. **Section 3.28: PROPOSAL TIMELINE:** The following lists the dates and activities associated with this Request for Proposal. Please be advised, these are tentative dates and are subject to change.
Release of RFP to proposers August 11, 2023
Deadline for proposers to submit questions August 25, 2023
Knox County responds to questions August 30, 2023
Proposals due into Procurement Division September 12, 2023 @ 2:00 p.m. eastern
Evaluations of proposals begin September 12, 2023
Presentations/Interviews, if needed September 18, 2023 – October 13, 2023
Evaluation process concludes September 28, 2023
Award Contract September 29, 2023
Contract Effective Date February 1, 2024

Question: The listed timeline only provides four months to stand up operations once the contract is awarded, including leasing buildings, buying ambulances, hiring, and onboarding employees, setting up the communications center, purchasing and installing so□ware systems, etc. Given that December is a "short" month due to the holidays, how is any vendor, other than the incumbent able to successfully meet that timeline?

Answer 4. As per Section 3.28, these dates are tentative and subject to change. It is the intent of the County for the Contract to begin February 1, 2024. However, the exact start date for the successful proposer to begin providing services will be determined in the final Contract as negotiated.

Question 5. **Section 3.33 - REMOVAL OF CONTRACTOR'S EMPLOYEES**: Contractor agrees to utilize only experienced, responsible, and capable people in the performance of the work. Knox County may require that the Contractor remove from the job covered by this Contract, including employees who endanger persons or property or whose continued employment under this Contract is inconsistent with the interest of Knox County.

Question: Please clarify this requirement. Will the County have the authority to fire or replace any employee at any time, based solely upon their request? Are there documented criteria used by the County to make those termination decisions?

Answer 5. This would be situation specific. An example of when this could happen would be Knox County Medical Director recommending suspending an employee based on unsafe or dangerous clinical practice.

Question 6. **Section 4.1 -SCOPE OF WORK:**

Schedule A: Emergency Medical Services

The awarded Contractor shall be responsible for providing Knox County Emergency Communications District (KCECD) with ambulance response to emergency requests throughout Knox County which are defined as Priority 1 Emergent Request, Priority 2 Urgent Request, and Priority 3 Low Acuity request, as well as additional associated support services such as behavioral health transports and decedent transports. The awarded Contractor will be exclusively responsible for providing all emergency responses and transports in Knox County. The awarded Contractor shall be responsible for furnishing vehicles with suitable supplies and equipment. All vehicles operated in conjunction with this service must be fully operational. The Contractor shall oversee fleet maintenance.

Questions:
- **Please specify the exact type of "behavioral health transport" that will be required.**
- **Do these transports include prisoner transports?**
- **Will transport to and from the County Jail be required?**
- **Please provide an anticipated number of these "behavioral health transports" and who will be responsible for management of these transports.**
- **Please specify the exact type of "descendent transports" that the Vendor will be responsible for handling.**
- **Will this include all transports for the County Coroner's Office?**
- **Please provide an estimated number anticipated.**
- **Who will be responsible for payment for these transports?**

Answer 6.

1. Any call coming in through 911 is required to be answered for response and or transport.
2. If ambulance transport is required.
3. If ambulance transport is required.
4. N/A
5. Most common decedent transport is from a scene. There are requests to transport from Hospital facilities.
6. Yes.
7. N/A
8. There is not a payor.

Question 7. **Section 4: The Contractor will not bill the County or the patient for transportation of those enrolled in the Indigent Care program**

Question: Please explain / describe the Indigent Care Program and how the program works.

Answer 7. The Knox County Indigent Care Program is a program created by Knox County to provide health care assistance to indigent population of Knox County. This program is funded by approval of the Knox County Commission on an annual basis. Knox County sets the eligibility requirements and the approved healthcare covered by the program. The actual enrollment is contracted to Cherokee Health Systems. In addition, Cherokee Health System provides all primary care for the individuals enrolled on the Indigent Care Program. Pursuant to Tennessee Code Annotated, Section 41-4-115(a), medical care of prisoners in the Knox County Jail and Corrections Facility are the responsibility of Knox County during the term of their incarceration. Primary care will be provided to prisoners directly by the medical staffs in the jail and corrections facility, with hospital care, testing which cannot be provided through the jail or correctional facility's clinic, and specialty physician care covered by the indigent care program.

Question 8. The County requires that only 911 operations occur within Knox County Emergency Communication District. If the EMS Contractor elects to connect their CAD to the County's CAD, the county would consider shared expense and connection within the first six months of service and retro back to the first day of the contract. Furthermore, all on- duty and off-duty units will be equipped with AVL and GPS data and shared with the County. The County encourages and will take under consideration, the proposing of alternate service delivery methods including, but not limited to, the incorporation of local area ALS First Responder Non-Transport groups, Mobile Integrated Healthcare Programs, and/or Healthcare Navigation and Quick Response Vehicle programs. Understanding that these groups play a vital role in the delivery of services to Knox County citizens, proposers shall submit information to incorporate each agency. Any proposed service delivery system which does not incorporate current ALS First Responders will be required to provide independent documentation/analysis that proposed system will meet County and State regulations and community standard of care.

Questions:

- **What if local area ALS First Responders do not want to be a part of the overall EMS System?**
- **Will arrival of local area ALS First Responders on scene "stop" or in any way change the response time standards of the RFP?**
- **Can the Vendor utilize BLS Transport ambulances to respond to Code 1 and Code 2 – 911 calls in coordination with local area ALS First Responders. / ALS First Response non transport units?**
- **Can the Vendor incorporate their own ALS First Response non transport units into their RFP proposal?**
- **Can the Vendor utilize BLS Transport ambulances to respond to Code 1 and Code 2 911 calls in coordination with their own ALS First Response non transport units?**

Answer 8.

1. The clock is related to the EMS Contractor and not the Medical First Responder.
2. There will need to be a Memorandum of Agreement between the contractor and Medical First Responder Agency with copy of the agreement provided to Knox County EMS Coordinator. There is not any requirement that another Medical First Responder Agency agree to do so.
3. Yes, however there will need to be a Memorandum of Agreement between the contractor and Medical First Responder Agency with copy of the agreement provided to Knox County EMS Coordinator.
4. Yes, you can propose what you would like, however the clock begins and ends with the correct transport capable unit arriving at location.
5. Yes.

Question 9. Successful proposer shall be required to make lease payments to Knox County Emergency Communication District (KCECD) for the ambulance dispatch of E-911 calls only. These payments will be made on an annual basis over the initial term of the Contract. Knox County intends all calls placed to E-911 to be dispatched utilizing APCO protocols. Not all calls to E-911 are emergency calls and shall be identified as such where applicable.

Questions:

- **APCO protocols allow for customization. Please provide the methodology of algorithm under which determination of Code 1, Code 2, and Code 3 calls are made? (Or will this methodology or algorithm be determined by the Vendor's Medical Director?)**
- **Please provide the methodology or algorithm under which determination of use of Healthcare Navigation and/or Mobile Integrated Healthcare Programs will be made? (Or will this methodology or algorithm be determined by the Vendor's Medical Director?)**
- **The International Academies of Emergency Dispatch currently has a very robust capability to triage emergency medical calls to determine both the correct response mode (Life Threatening Emergency vs Non-Life Threatening); correct level of care (ALS vs BLS) as well as determinants for proper use of Healthcare Navigation and/or Mobile Integrated Healthcare Programs in its MPDS Dispatch System. This system is heavily supported by extensive research data. Would the County consider the utilization of the MPDS System instead of APCO?**

Answer 9.

1. The vendor Medical Director and Knox County's Medical Director can partner on the methodology of algorithm, but final approval comes from Knox County's Medical Director.
2. In Collaboration with Knox County's Medical Director under the Pilot Clause.
3. Not unless the vendor wishes, at their cost, to pay for both the installation, training, maintenance, etc...as well as any cost of county personnel time and software connection. Any system will stay with Knox County if vendor ever exits.

Question 10. Contractor will be required to utilize a County approved and owned operational and clinical performance software and pay for utilization of the service.

Question: Please specify exact operational and clinical performance software required.

Answer 10. First Watch OCU and First Pass is the County's preference. Vendors may propose another nationally recognized software solution.

Question 11. At the contractor's expense, The County will hire the EMS Systems Medical Director that the EMS contractor must use for clinical oversight. Contract will be allowed to deploy a tiered response system allowing for the Medical Director to set the acuity based on the APCO cards and the Contractor to deploy the proper resource type that will meet the patient's needs and performance standard.

Questions:

- **APCO protocols allow for customization, can you please provide methodology or algorithm under which determination of Code 1, Code 2 and Code 3 Calls will be made? (Or will this methodology or algorithm be determined by Vendor's medical director?)**
- **Please provide methodology or algorithm under which determination of use of Healthcare Navigation and/or Mobile Integrated Healthcare Programs will be made? (Or will this methodology or algorithm be determined by Vendor's medical director?)**
- **The International Academies of Emergency Dispatch currently has a very robust capability to triage emergency medical calls to determine both the correct response mode (Life Threatening Emergency vs Non-Life Threating); correct level of care (ALS vs BLS) as well as determinants for proper use of Healthcare Navigation and/or Mobile Integrated Healthcare Programs in its MPDS Dispatch System. This system is supported heavily by extensive research data. Would the County consider the utilization of the MPDS System instead of APCO?**
- **Can the Vendor utilize BLS transport ambulances to respond to Code 1 and Code 2 - 911 calls in coordination with local area ALS First Responders ALS First Response non transport units?**
- **Can the Vendor incorporate their own ALS First Response non transport units into their proposal to the RFP?**
- **Can the Vendor utilize BLS transport ambulances to respond to Code 1 and Code 2 - 911 calls in coordination with their own ALS First Response non transport units?**

Answer 11. See answers 8 and 9.

Question 12. Decedent transport services can utilize any unit needed to meet the performance timeframe to include a single provider in a transport van with proper equipment and stretcher.

Questions:
• Please specify exact type of "decedent transports" that Vendor will be responsible for?
• Will this include all transports for the County Coroner's Office? Please provide anticipated number of transports.
• Who will be responsible for payment for these transports? What certification level must the "provider" have?

Answer 12. See answer 6.

Question 13. **Section 4.2 - GOALS OF THE PROCUREMENT:** Ambulance service is one component for the provision of effective medical services in the community. This RFP seeks proposals for 911 ambulance service for Knox County, TN.

If in any year, the successful contractor requests a subsidy, the final operating agreement shall contain language requiring the contractor to provide audited financial statements, for their local legal entity, and to the degree required, similar supporting documentation for the parent company, as defined in the final operating agreement. Any requested subsidy shall not result in an operating net balance of more than 12%.
Questions:
• Does this mean the county will accept a request for subsidy for the RFP?
• Please clarify what the County considers "Operating Net Balance."

Answer 13.

1. Yes.
2. As defined in Section 4.2 Any requested subsidy shall not result in an operating net balance of more than 12% profit.

Question 14. **Section 4.5 SIGNIFICANT EMS SYSTEM ENHANCEMENTS:** The County supports an EMS System focused on quality patient care, provider financial stability, and quality training for all EMS providers. Although Knox County has a solid foundation in this regard, this RFP is an opportunity to improve systems of care including:

A. Clinical Metrics and Liquidated Damages The goal of the County is to provide a clinically sophisticated system that achieves contemporary benchmarks of clinical excellence and can continue to do so in a sustainable fashion. These system specifications are drawn from many reference sources but are generally consistent with the direction provided in the National Highway Traffic Safety (NHTSA) document, The EMS Agenda 2050, and are consistent with core recommendations of the Institute for Medicine report on EMS: Emergency Medical Services: At the Crossroads.

To facilitate the routine and progressive oversight of the clinical aspects of the EMS System, Knox County will develop clinical Key Performance Indicators (KPIs) and a Clinical Scoreboard. These will be utilized to either assess financial credits or levy response time liquidated damages based on the Contractors clinical performance.

Monthly Compliance will determine if clinical performance credits and/or performance penalty(s) will be applied to the Contractor as further defined below.

Questions:
• Can you please specify exact Clinical KPI's, how they are to be tracked and audited?
• Can you please specify the number of financial credits or reductions in liquidated damages per Clinical KPI?

Answer 14.

1. The providers protocols that are associated with Code Heart, Stroke, Trauma, etc.
2. Refer to chart in 5.3 of RFP.

Question 15. **Section 4.6 - RELEVANT INFORMATION REGARDING SERVICE AREAS:** The County specifically makes no promises or guarantees concerning the number of emergency calls or transports, quantities of patients, or distance of transports that are associated with this procurement. Every effort has been made to provide accurate information, but the Proposers are to use their professional judgment and expertise to develop their economic and operational plans and proposals.

Annual Response and Transport Volume					
2018	**2019**	**2020**	**2021**	**2022**	
Total Responses	59,152	60,461	62,242	65,237	63,927
Total Transports	44,248	43,751	43,237	43,932	43,281
Average Loaded Miles	N/A	N/A	N/A	N/A	8.1

Questions:
- **In order to complete an accurate System Status Plan, detailed response and transport data must be analyzed. Can you please provide the following response and transport data for the service area in electronic format.**
- **Can you please provide 2023 data to date.**
- **Does above listed data include "Behavioral Health" transports?**
- **Does above listed data include "Decedent" transports?**

Answer 15. Proposers must email Jay Garrison with the Knox County Procurement Division at jay.garrison@knoxcounty.org to receive a copy of the Fitch Associates Consultant Report which details the data requested.

Question 16. **Section 4.6 Current System Performance** The current Contractor has recently struggled to meet the County response time requirements over the term of the contract and subsequent extensions. Calendar year 2022 has represented an unusual year given a variety of factors. As such, the County has elected not to include this data, given the wild variation from the previously established norms.

Question: **Do you mean 2023 Data? 2022 data is shown. Can you please provide 2023 data to date?**

Answer 16. See answer 15.

Question 17. **EMS Independent Annual Audit** The County has the option to require an Independent Audit solely at its discretion and at the contractor's cost.

Questions:
- **Would this be a financial audit, an operational audit or both?**
- **Under what circumstances would this audit be triggered?**

Answer 17. Annual operations and financial review. It is at the discretion of County, there are not any defined parameters.

Question 18. **Section 5.3 CLINICAL PERFORMANCE MEASUREMENT AND INCENTIVE:** To maintain routine high-quality EMS Services, the clinical performance of the Contractor's quality of care provided to the patients will be routinely measured. The Contractor shall work with Knox County to develop an electronic reporting method for clinical metrics. Data submission platform shall show clinical metrics in real-time. The Clinical Scorecard (Appendix 3) outlines both Core and Revolving Clinical KPIs.

The Core KPIs are considered to have a more direct impact on the health and safety of patients within the EMS system, these metric categories (STEMI, Stroke, Trauma, Cardiac/Respiratory Arrest) will remain unchanged throughout the duration of the subsequent agreement. Changes may be made with mutual agreement between Knox County and Contractor. The revolving KPIs are to be driven by routine CQI data. These will be adjusted on a quarterly basis as needed. Refer to section 6.8 Response Time Exceptions and Exemption Requests.

The County's commitment to the Triple Aim approach, is demonstrated by utilizing the Contractor's clinical performance as a key contract compliance measurement tool. Based on the Contractor's clinical performance the County will either provide a future financial credit on response time compliance liquidated damages or levy liquidated damages for clinical performance. The County intends to provide a monthly Clinical Scorecard, outlining the Contractor's performance in all clinical measures, as well as tabulating a weighted total compliance value for all clinical KPIs.

Questions:
- **Can you please specify exact Clinical KPI's, how they are to be tracked and audited?**
- **Can you please specify the number of financial credits or reductions in liquidated damages per Clinical KPI?**

Answer 18. See answer #14.

Question 19. During the vendor's monthly compliance meeting clinical performance will be weighted to be used as a credit for monthly time response penalties.

Overall Weighted Clinical Performance	Credit
90 – 94.9%	*45%*
95 – 97.4%	*50%*
97.5 – 100%	*65%*

Questions:
- **Can you explain how the credit to monthly response time penalties is to be applied?**
- **Is credit percentage to be applied to the dollar amount of response time penalties?**

Answer 19.

1. Example: If time penalties were assessed at $1000.00 and clinical performance was rated between 95-97.4% then 50% credit would be applied to the $1,000.00 fine bringing fine to $500.00.
2. Yes.

Question 20. For clinical performance under 80% (used for illustrative purposes in the Clinical Scorecard), Knox County may levy, and the Contractor shall pay Knox County liquidated damages for each month that the Contractor fails to comply with ANY core clinical quality measure, as outlined in the clinical scorecard.

Question: What is the level of liquidated damages?

Answer 20. See 5.4 of the RFP.

Question 21. **Section 5.4 -LIQUIDATED DAMAGES PROVISIONS FOR CLINICAL PERFORMANCE:** Isolated instances of individual deviations of clinical performance standards may be considered instances of minor non-compliance with the Agreement. However, deviations of clinical performance standards, which are severe or chronic, may constitute a Default of the Agreement as defined by these specifications.

Failure to comply with any clinical performance metric or other requirements in this RFP or the final Contract will result in damage to the County. Therefore, the Contractor and the County agree to the liquidated damages specified herein. It is expressly understood and agreed that the liquidated damages amounts are not to be considered a penalty but shall be deemed taken and treated as reasonable estimate of the damages to Knox County.

Question: What is the level of liquidated damages?

Answer 21. Same as answer 20.

Question 22. It is also expressly understood and agreed that Knox County remedies in the event of the Contractor's breach or any noncompliance, are not limited to this RFP or the final Contract liquidated damages provisions. Chronic failure to comply with the clinical performance requirements may constitute breach of contract.

Outlined in the Clinical Scorecard in Appendix X3 are the Clinical Performance metrics for which Knox County will levy liquidated damages and consider the Contractor in breach based on a fore mentioned performance. These damages will be assessed monthly.
• Level 1 non-compliance will result in a $1500.00 damage per metric, per month.
• Level 2 non-compliance will result in a $3000.00 damage per metric, per month.
• Compliant (eligible for credit) 90% or greater
• Compliant (damages apply) 80% - 89.99%
• Level 1 non-compliance 75 - 79.99%
• Level 2 non-compliance 74.99% or less

The Contractor will be required to conduct a comprehensive performance improvement process and submit it to the County within 10 days following the identification of underperformance for two consecutive months. The County will review and provide further recommendations as necessary prior to the approval of any proposed corrective action, to include adjustments to the system status plan or other measures to comply with the 90% requirement.

Question: Please provide further explanation regarding the scorecard, calculations, and how the data is utilized?

Answer 22. Performance percentages are Key Performance Indicators (KPI) based on response codes categories such as: Heart, Stroke, Trauma.

Question 23. **Section 6.1 - PERFORMANCE CONTRACT AND REVIEW:** The most important aspect of this procurement is the fact that this procurement will result in the award of a ***performance contract***. This procurement requires the highest levels of performance and reliability, and the mere demonstration of effort, even diligent and well-intentioned effort, shall not substitute for performance results. A contractor who fails to perform must and shall be promptly replaced, because human lives, and not merely inconvenience or money, are at stake.

- Ambulance response times must meet the response time requirements set forth in the summary of response times requirements, Figure 1 attached hereto.
- Every ambulance unit must at all times be equipped and staffed to operate at the ALS level (Paramedic) or Critical Care level (CCEMTP), on all emergency calls received from the Knox County Emergency Communications District.

Questions:
• What if local area ALS First Responders do not want to be part of the overall EMS System?
• Will arrival of local area ALS First Responders on scene “stop the clock” or in any other way change the response time standards of the RFP?
• Can the Vendor utilize BLS transport ambulances to respond to Code 1 and Code 2 911 calls in coordination with local area ALS First Responders ALS First Response non transport units? • Can the Vendor incorporate their own ALS First Response non transport units into their proposal to the RFP?
• Can the Vendor utilize BLS transport ambulances to respond to Code 1 and Code 2 911 calls in coordination with their own ALS First Response non transport units?

Answer 23. Same as Answer #8.

Question 24. Clinical performance must be consistent with Nationally Accredited medical standards and best practices with annual reviews of protocols and standing orders by Medical Director.

Question: Please specify the source of the *nationally accredited medical standards being referenced.*

Answer 24. Based on Knox County Medical Director expectations.

Question 25. **Section 6.4 - RESPONSE TIME PERFORMANCE REQUIREMENTS:** These specifications outline three (3) priorities with which Contractor must comply by meeting specified Response Times. The call classification as Priority 1 through 3 is accomplished by presumptive APCO prioritization by the County Designated Communications Center. For response time monitoring, reporting and compliance purposes, within the County, Contractor's response time on requests for ambulance service originating from within the service area shall meet the following performance standards.

Questions:

- APCO protocols allow for customization, can you please provide methodology or algorithm under which determination of Code 1, Code 2 and Code 3 Calls will be made? (Or will this methodology or algorithm be determined by Vendor's medical director?)
- APCO protocols allow for customization, can you please provide methodology or algorithm under which determination of use of Healthcare Navigation and/or Mobile Integrated Healthcare Programs will be made? (Or will this methodology *or algorithm be determined by Vendor's medical director?)*

Answer 25. Same as answer #9.

Question 26. D -Summary of Response Time Requirements - Figure 1 summarizes the Response Time Compliance requirements for ambulances throughout the County by Priority and Zone.

Zone	**Priority Level**	**Compliance**	**Performance Standard**
City (Incorp)	Priority 1	90%	≤10:00
Priority 2	90%	≤15:00	
Priority 3	90%	≤ 30:00	
Zone	**Priority Level**	**Compliance**	**Performance Standard**
East	Priority 1	90%	≤20:00
Priority 2	90%	≤25:00	
Priority 3	90%	≤ 30:00	
Zone	**Priority Level**	**Compliance**	**Performance Standard**
West	Priority 1	90%	≤20:00
Priority 2	90%	≤25:00	
Priority 3	90%	≤ 30:00	
All Field Service Areas	**Deceased Patients**	**90%**	**≤ 45:00**

Question: Can you provide a precise map and written description for the geography of each Zone

Answer 26. See Answer 15.

Question 27. **Section 7.3 VEHICLES AND EQUIPMENT:** Contractor shall acquire and maintain all ambulances, support vehicles, on-board medical supplies/equipment and office facilities and equipment to be used by Contractor to perform its services under the Agreement. All costs of maintenance including parts, supplies, spare parts, and costs of extended maintenance agreements shall be the responsibility of the Contractor.

A. Ambulances

All ambulances shall meet federal and state requirements as outlined in all applicable Tennessee State Statutes and Regulations. Proposers shall articulate their intended fleet that can conform to the following requirements:

1. Ambulances may be standard Type I or Type III for ALS and or BLS use, Type II for BLS only.
2. Be identically configured with the capability to carry all supplies necessary to function in accordance with Knox County Ordinance.
3. Contractor shall, at a minimum, maintain an unstaffed but fully equipped Bariatric capable ambulance with the capability to transport patients with communicable diseases, within the County and be able to immediately staff the unit and provide these services within a reasonable time frame should they become necessary.
4. Contractor shall have a mechanism to monitor driver safety.
5. Ambulances shall be limited to a maximum mileage of 300,000 miles and/or no more than seven (7) years old, in the event there are delays in end-stage ambulance manufacturer or remounting production time, the Contractor can request an exception from Knox County.
6. Supervisor and other support vehicles shall be limited to a maximum of 300,000 miles.
7. No more than 50% of the ambulance fleet shall have over 150,000 miles at the start of the contract. A list of all vehicles detailing make, model, age, and maintenance records must be provided to Knox County.
8. Contractor shall maintain a fleet of ambulances that meets or exceeds 130% of the peak level of deployment as determined by the Fitch and Associates Consultant Report procured by Knox County, TN.

Question: **What is the fleet level that exceeds 130% of peak level deployment as determined by Fitch and Associates Consultant Report?**

Answer 27. FITCH's review had ALS Peak of Day at 15 during specific days of the week and BLS Peak of Day at 4. This is a starting point. The Fitch Report is available as per Answer 15.

Question 28. **Section 8.3 CUSTOMER SERVICE HOTLINE AND COMPLIANCE PROCESS**: C - Members of the Contractor's Leadership Team are to be automatically notified via pager/text message of any incoming calls. A management designee must return the call to the customer within 30 minutes, 90% of the time. Incidents that require feedback are to be attended to by the end of the next business day.

Question: **Is the 30-minute response to be 24/7/365?**

Answer 28. Per the RFP, a manager designee is allowed, and the County would assume there will always be a manager or supervisor on duty that could be designated to do this.

Question 29. **Does the contract include inter-facility transport (IFT)? The service level data indicates 0% for ALS non-emergency and BLS non-emergency, yet payor mix data includes hospitals as payors (1%) which seem to indicate IFT (Medicare part A stays for example).**

Answer 29. Hospitals and healthcare facilities arrange their own IFTs. That was based on a few patients in the data set from the current vendor, based on 911 call for hospital IFT.

Question 30. **Is payor data available that is more reflective of transports covered by this RFP?**

Answer 30. Payor mix in RFP section 4.6 is all that is available.

Question 31. **Does "private pay" include indigent care as discussed in RFP?**

Answer 31. Yes.

Question 32. **Section IX Proposal Format:**

Question: Under Tab II: General Information, the instructions indicate to include a one-page cover letter. Is this a separate cover letter from the one that is required in Tab I: Table of Contents and a Cover Letter? If the two are the same, does the letter need to be contained within one page, or can it run longer?

Answer 32. These are the same. Please provide one cover letter under Tab II. The County does request this cover letter be limited to one page. Details of the proposer's capabilities should be contained in their response. Proposers shall also provide a separate statement authorizing the submittal of the proposal, which shall be signed by a representative of the company that is authorized to bind the company.

Question 33. **Attachment A**

Line 6 - **Question: Please confirm what type and/or line of coverage being requested that would be different than contained in standard GL and/or PL policies?**

Line 7 - **Please confirm if a separate limit is required for Contractual Liability or if standard Contractual Liability coverage contained in ISO General Liability policies is sufficient?**

Answer 33. **T**he standard in GL and/or PL policies is what the County is asking for.

The standard Contractual Liability coverage is sufficient.

Also note that the requirements of the insurance coverage have been amended from what was released in Addendum I.

Question 34. **Due Diligence/Data Questions -** The following information is requested as part of our initial due diligence prior to coming on site.

Service Area Information

- Map of service area to Identify services provided in each geographical area
  - o Identify service area(s) / boundaries if they do not align with county / municipality boundaries

- List of each fixed station (include stations owned, leased, or shared) o Street address
  - o City
  - o Zip code
  - o Longitude and Latitude or X and Y coordinates
  - o Number and type of vehicles deployed from the station
  - o Area covered by the station

- If applicable, list of each flexible deployment post location o Street address
  - o City
  - o Zip code
  - o Longitude and Latitude or X and Y coordinates
  - o Area covered by the post

- On scene response volume, by level / type of service, in monthly increments for the past three years by service type (Emergency ALS, Emergency BLS, Non-emergency ALS, Non-emergency BLS, SCT, etc.)

Encounter / Incident Information

- Three to five years' worth of data for each operating area o Unique identifier – encounter / incident number
  - o Date of the encounter / incident
  - o Longitude and Latitude or X and Y coordinates of encounter / incident
  - o Street address of encounter / incident
  - o City of encounter / incident
  - o State of encounter / incident
  - o Zip code of encounter / incident
  - o Dispatch Zone (or contract are or first due station)
  - o Unit ID
  - o Type of call (Emergency Non-Emergency)
  - o Resource Needed (ALS or BLS or CCT or Neonatal CCT)
  - o Resource Sent (ALS or BLS or CCT or Neonatal CCT)
  - o MPDS triage / dispatch code / chief complaint
  - o Call priority
  - o Encounter / Incident disposition (e.g., Cancel reason, transported, etc.)
  - o Date/Time call received by PSAP
  - o Date/Time call received by dispatch center
  - o Date/Time transport service requested (request for non-emergency transportation services)
  - o Date/Time of dispatch
  - o Date/Time en route
  - o Date/Time arrived on scene
  - o Date/Time departed scene
  - o Date/Time arrived at destination
  - o Date/Time cleared destination
  - o Date/Time cancelled
  - o Transport destination (facility name or address)

Revenue Cycle / Billing information

- 3 – 5 Years Granular Billing Data
  - o Unique encounter / incident identifier
  - o Date of the encounter / incident
  - o Type of transport indicator (level of service)
  - o Point of origin
  - o Point of pick-up address
  - o Point of pick-up city
  - o Point of pick-up State
  - o Point of pick-up zip code

o Emergency indicator
o Insurance Payor / Payor class
o Date claim submitted
o HCPCS codes / ICD9 Code
o Gross charges
o Deductions / contractual allowances
o Amount paid
o Date of denial if applicable
o Date denial contested / additional information provided
o Date claim paid
o Amount paid by primary insurer
o Amount of patient responsibility / secondary insurer
o Date billed to patient / secondary insurer
o Date patient / secondary insure paid
o Amount paid by patient / secondary insurer
o Date sent to collections - if applicable
o Amount of any balance write-offs
o Date of balance write-off

• Listing of rates by level of service
• Provide any payor contracts / agreements
• Please provide random samples of 50 recent transports with billing sheets associated with the call plus all supporting documentation (e.g., PCS). Please include PCR and provide good distribution between Emergency, Non-emergency, and LOS

Staffing
• An organizational chart o Include each job title / function and delineate the reporting structure
o Include the number of FTE(s) for each position
o Include the number headcount of the number full-time and part-time persons working in each position

• Copies of all unit work schedules o Days of the week the crew / shift works
o Hours the crew / shift works each day
o Staffing configuration for the crew / shift
• Number of paid time off hours by level of certification for the past year
• Number of hours worked by Part Time / PRN staff for the past year
• Provide data on FT employees including number of staff by title, pay rates, benefits & tenure
• Confirm compliance and provide copies of inquiries or investigations with all EEOC, FSLA, ADA, Affirmative Action, and any other regulatory requirements.
• Provide copies of any outstanding or anticipated litigation related to employment matters.
• Provide copies of any Collective Bargaining Agreements.

Contract Matrix
• List of each contract to include the following information: o Covered services or type of services provided
o Geographical area to which the contract pertains
o Reimbursement rates / discounts provided
o Contract expiration dates
o Exclusivity

• Provide copies of all EMS agency service provision contracts

Financial
• Three to five years of financial statements o Organizational roll-up
o Service or contract level profit and loss statements as granular as possible
o Detailed expense line and revenue data as granular as possible (by category)

Operational
• Policies & Procedures o Please provide a copy of all operational policies and procedures, guidelines, etc.

• Clinical Protocols o Please provide a copy of all clinical protocols used by the organization

• Fleet o Provide a list of all vehicles, VIN's, Year, Mileage, Owned/Leased, and any outstanding amounts due.

• Risk Management to Provide copies of all Safety/Risk policies
o Provide copies of Loss Runs for all lines of Insurance for the past five years
o Provide information about any current or anticipated liability or workers compensation litigation valued at $10,000 or more.
o Provide copies of any regulatory inquiry or investigation
o Provide copies of all insurance policies

• Procurement o Provide a list of all current suppliers and spend by category
o Provide copies of any agreements with vendors or Group Purchasing Organizations.

• Legal
o Provide a summary of the Organization Structure
o Provide descriptions of a current or anticipated litigation valued at $10,000 or more.

Answer 34. See Answer 15.

Question 35: In RFP Section IX, Proposal Format, Knox County requests that TAB I contain the cover letter (page 32). Then, it also requests that the cover letter be included in TAB II. Can Knox County advise on the appropriate formatting and/or placement of the cover letter?

Answer 35: See Answer 32.

Question 36: RFP Section I, General Terms and Conditions, 1.21 states, "Vendors must complete the proposal forms contained in the proposal package. Failure to complete the proposal forms may result in proposal rejection." Can you clarify which forms this requirement refers to? AMR did not find any forms in your RFP save for Attachments A, C, and D.

Answer 36: As revised per Question 37, Attachments A, B, and C are required to be submitted with your response.

Question 37: The Attachments provided by Knox County go from A to C and D. Can you confirm the absence of Attachment B?

Answer 37: The attachment labels have been corrected. See attached.

Question 38: RFP Section IV – Scope of Services, 4.1, Scope of Work, Schedule A: Emergency Medical Services states the Contractor will be responsible for "additional associated support services such as behavioral health transports and decedent transports". Are behavioral health and decedent transports included in the total transport volume provided by Knox County? If so, can you provide a breakdown of when those calls occur as well as if the transports are from the scene or the hospital?

Answer 38: These are based on Scene calls not hospital transports.

Question 39: RFP Section IV – Scope of Services, 4.2, Goals of the Procurement states, "Any requested subsidy shall not result in an operating net balance of more than 12%." Can Knox County define the calculation or formula for the net operating balance? What happens in the event the operating net balance ends up being more than 12%?

Answer 39: If subsidy is proposed no more than 12% of the tax payor subsidy involved, the County will then reduce the subsidy to a max of 12% profit for the vendor.

Question 40: In regard to the requirements posed in Section 6.4, Response Time Performance Requirements in the RFP, understanding that the average Emergency Department (ED) offload delay is approximately sixty (60) minutes, will there be any exceptions for response delays due to extended wall times?

Answer 40: Exceptions can be proposed by the vendor on how they wish to handle both from an operations perspective and a calculation methodology.

Question 41: Section 7.3 -Vehicles and Equipment, A (Ambulances) #8 of the RFP states, "Contractor shall maintain a fleet of ambulances that meets or exceeds 130% of the peak level of deployment as determined by the Fitch and Associates Consultant Report procured by Knox County, TN." Will a copy of the EMS Fitch & Associates report be provided?

Answer 41: See Answer 15.

Question 42: Will the Contractor be allowed to continue providing non-emergency dispatch within the Knox County Emergency Communications District (KCECD)?

Answer 42: Only calls coming through 911.

Question 43: Understanding the RFP requires a Paramedic for all ALS response, would the County consider an EMT Advanced (EMT-A) and an EMT Basic (EMT-B) as an ALS response in accordance with new State regulations?

Answer 43: Knox County's expectation is all Priority 1 (life Threatening responses) have a paramedic unit stop the clock.

Question 44: Section 5.3 states that the clinical scorecard is for illustrative purposes. Does that mean the parties will jointly develop the final clinical metrics?

Answer 44: Knox County medical director has ultimate oversight.

Question 45: In reference to Section IX - Scoring Guidelines, can Knox County provide a breakdown of how points for Part IV: Cost will be calculated?

Answer 45: Cost is subsidy break down.

Question 46: How are the lease payments to Knox County Emergency Communications District (KCECD) calculated? Can you provide a cost breakdown? Will the County own the equipment at the console, or will that be at the expense of the Contractor?

Answer 46:

- Square footage in the communications center
- The sit-stand dispatch console, including warranty and any service work needed
- 8 monitors used on the consoles
- 24/7 Chair
- Redundant power/wireless internet
- Technical 911 CAD Network and GIS Assistance
- Use of kitchen, respite facilities, training space
- We would allow use on our fiber ring pending cyber security agreements

KCECD monthly fees would not cover the following:

- Computers needed to dispatch and call handling
- Console radios for EMS Dispatch (we own the system and maintain all the sites in conjunction with the TN Valley Radio Communications System)
- Any headsets or auxiliary equipment needed by vendor employees

KCECD would also be able to facilitate EMS dispatch services for the vendor at a price of approximately $900,000 annually.

Question 47: Can you provide the average net collectible per transport for the county?

Answer 47: We cannot because we are allowing the vendors to propose their own charge master rates if they would like. Current vendor is below the RFP proposed 300% Medicare allowable.

Question 48: Can you provide the Top 3 Payors for Medicare HMOs?

Answer 48: Knox County does not have this information.

Question 49: Can you provide who the top 3 Commercial Payors are for the county?

Answer 49: See answer 48.

Question 50: Is there a currently a subsidy being provided? If so, can you provide what that currently is?

Answer 50: There is currently not a subsidy.

Question 51: Currently on average how many ambulances are required to manage the system?

Answer 51: The current contract does not require a specific number of ambulances. The Fitch Report is available as Per Answer 15.

Question 52: Currently on average, how many field supervisors are required to manage the system daily?

Answer 52: Vendors sets this, not the county.

Question 53: Request a copy of Knox County Information Technology (KCIT) enterprise security policies and requirements.

Answer 53: Knox County INFORMATION SECURITY Management Policy has been attached.

Question 54: How much is the First Watch licensing and annual fees as required?

Answer 54: Licensing for all compliance tools including First Watch and First Pass will average around $143,000.00 the first year and then $79,000.00 each year after.

Question 55: How much is the First Pass licensing and annual fees as required?

Answer 55: Same as answer #54.

Question 56: How much is the Patient Centric View Interactive Dashboard (IDV)?

Answer 56: Same as answer #54.

Question 57: How much is the Online Compliance Utility (OCU)?

Answer 57: Same as answer #54.

Question 58: **Re: Section 2, 2.22, "TERMINATION", on page 5:** With the sizable investment of capital resources and dollars to fulfill the requirements, would the County consider termination for cause only?

Answer 58: See Answer #1.

Question 59: **Re: Section 3, 3.2, "ACCEPTANCE", on page 6:** Vendors are advised that the payment of an invoice does not necessarily constitute as an acceptance of services that are provided. Acceptance requires a specific written action by Knox County so stating.
a. Would the County detail what invoices it would be responsible to pay?

Answer 59: There are no invoices the county would be responsible for paying.

Question 60: **Re: Section 4, 4.1, bullet #1, "SCOPE OF WORK", on page 10:** Is there a financially responsible party for behavioral health and decedent transports? If so, what is the reimbursement rate? In addition, what percentage of responses and transports are behavioral health only or decedent?

Answer 60: There is not.

Question 61: **Re: Section 4, 4.1, bullet #2, "SCOPE OF WORK", on page 10:** Is there a responsible party for patients enrolled in the Indigent Care Program or is the bill completely written off? What percentage of transports does this section apply to?

Answer 61: See answer 60. Percentage not available

Question 62: **Re: Section 4, 4.1, bullet #6, "Communication Equipment and Costs", on page 11:** How many consoles are allocated to the ambulance provider, how many square feet in the dispatch center, and how many data racks?

Answer 62: The vendor would determine the number needed.

Question 63: **Re: Section 4, 4.1, on page 11:** The County encourages and will take under consideration, the proposing of alternate service delivery methods including, but not limited to, the incorporation of local area ALS First Responder Non-Transport groups, Mobile Integrated Healthcare Programs, and/or Healthcare Navigation and Quick Response Vehicle programs.

a. Would the County provide detail on any current alternate service delivery methods in use today?
b. Is any compensation currently provided to

Answer 63: Current vendor utilizes Nurse Navigation, QRV, ET3. The county does not currently pay a subsidy.

Question 64: **Re: Section 4, 4.1, on page 11:** Can the county identify the approved and owned operational and clinical performance software? What is the cost?

Answer 64: The county intends to utilize First Watch and First Pass. Other nationally recognized solutions can be proposed and considered. Cost see answer #54.

Question 65: **Re: Section 4, 4.2, on page 12:** Can the County advise what the current subsidy provided is?

Answer 65: The county does not currently pay a subsidy.

Question 66: **Re: Section 4.6, "RELEVANT INFORMATION REGARDING SERVICE AREAS", on page 13:** Can the County confirm if decedent, indigent, and behavioral health responses and transports are included in the table?

Answer 66: Yes.

Question 67: **Re: Section 4, 4.7, "DISPATCHING MODELING", on page 14:** a. Can the County elaborate on the statement "You must provide the subsidy, if any, for two dispatch models in your proposal."? What does "subsidy" refer to?

Answer 67: If the vendor is proposing a subsidy, you must provide the subsidy proposed for each model.

Question 68: **Re: Section 6, 6.1, "PERFORMANCE CONTRACT AND REVIEW", on page 17:** States every ambulance must be equipped and staffed at the ALS level or Critical Care level (CCEMTP) on all emergency calls, but Priority 3 calls can be BLS staffed. Can the County please confirm that BLS ambulances can be used in the 911 system for low acuity calls?

Answer 68: Yes

Question 69: **Re: Section 6, 6.7.A, "Documentation of Incident Time Intervals", on page 21:** *Contractor shall document all times necessary to determine total ambulance response time. All times shall be recorded on the Knox County approved Patient Care Report (PCR).*

a. Would the County please provide the current and preferred (if different) ePCR platform?

Answer 69: The vendor supplies the ePCR.

Question 70: **Re: Section 7, 7.3 D. 8., "EQUIPMENT", on page 25:** a. What is the current and preferred (if different) cardiac monitor being used in the system?

Answer 70: The vendor supplies State Office of EMS approved equipment.

Question 71: **Re: Section 7, 7.4 A. 2., "Ambulance Communication Equipment", on page 25:** a. Can the county provide the current portable and mobile radio make and model for system interoperability?

Answer 71: The County does not have this information.

Question 72: **Re: Section 7, 7.8 , "TREATMENT OF INCUMBENT WORKFORCE", on page 27:** In this section, the County asks bidders to "offer all full-time employees a benefit program comparable to, or better than, the program offered by the incumbent provider." and that its goal is to "to ensure that the Contractor initially and throughout the term of the Agreement provides a financial benefit to encourage employee retention and recruitment for the system.". To ensure bidders meet these criteria, can the County provide the following:
a. Current salary and benefit information for the current workforce?
b. Number of EMTs and paramedics that are currently employed by the incumbent?

Answer 72: The County does not have this information. However, 7.8 also states "Awarded proposer will make a best effort".

Question 73: **Re: Response and Transport Data**: If possible, will the County and/or Knox County Emergency Communications District (KCECD) provide the following data points for each ambulance response and transport in 2019, 2020, 2021, &2022?
a. Incident ID& response ID
b. Pick-up address or latitude& longitude
c. Date dispatched
d. Time dispatched
e. Time at scene
f. Time transporting
g. Time at hospital
h. Destination latitude& longitude or address
i. Time back in service
j. Cancellation time
k. Assigned unit
l. Compliance zone (i.e., City, East, and West)
m. Level of service (i.e., BLS or ALS)
n. Transport (Y/N)
o. Priority code at time of dispatch

Answer 73: See answer 34.

End of Addendum II.

Jay Garrison, CPPO, CPPB
Procurement Coordinator
Knox County Procurement Division

This addendum is issued from the Knox County Procurement Division, Suite 100, 1000 North Central Street, Knoxville, TN 37917. The telephone number is 865.215.5777 and the fax number is 865.215.5778.

ATTACHMENT A
KNOX COUNTY PROCUREMENT DIVISION
INSURANCE CHECKLIST
PROPOSAL NUMBER 3454

THE CERTIFICATE OF INSURANCE MUST SHOW ALL COVERAGES & ENDORSEMENTS WITH "YES" AND ITEMS 20 TO 23

REQUIRED	NUMBER	TYPE OF COVERAGE	COVERAGE LIMITS	
YES	1.	WORKERS COMPENSATION	STATUTORY LIMITS OF TENNESSEE	
YES	2.	EMPLOYERS LIABILITY	$100,000 PER ACCIDENT $100,000 PER DISEASE $500,000 DISEASE POLICY LIMIT	
YES	3.	AUTOMOBILE LIABILITY X ANY AUTO-SYMBOL (1)	COMBINE SINGLE LIMIT (Per -Accident)	$ 5,000,000
			BODY INJURY (Per –Person)	
			BODY INJURY (Per-Accident)	
			PROPERTY DAMAGE (Per-Accident	
YES	4.	COMMERCIAL GENERAL LIABILITY		LIMITS
		CLAIM MADE / X / OCCUR	EACH OCCURRENCE	$3,000,000
			FIRE LEGAL LIABILITY	$100,000
			MED EXP (Per person)	$5,000
		GEN'L AGGREGATE LIMITS APPLIES PER	PERSONAL & ADV INJURY	$1,000,000
		POLICY / X / PROJECT / LOC	GENERAL AGGREGATE	$5,000,000
			PRODUCTS-COMPLETED OPERATIONS/ AGGREGATE	$2,000,000
YES	5.	PREMISES/OPERATIONS	$1,000,000 CSL BI/PD EACH OCCURRENCE $2,000,000 ANNUAL AGGREGATE	
YES	6.	INDEPENDENT CONTRACTOR	$1,000,000 CSL BI/PD EACH OCCURRENCE $1,000,000 ANNUAL AGGREGATE	
YES	7.	CONTRACTUAL LIABILITY (MUST BE SHOWN ON CERTIFICATE)	$1,000,000 CSL BI/PD EACH OCCURRENCE $1,000,000 ANNUAL AGGREGATE	
NO	8.	XCU COVERAGE	NOT TO BE EXCLUDED	
YES	9.	UMBRELLA LIABILITY COVERAGE	$10,000,000	
		PROFESSIONAL LIABILITY		
NO	10.	ARCHITECTS &ENGINEERS	$1,000,000 PER OCCURRENCE/CLAIM	
NO		ASBESTOS & REMOVAL LIABILITY	$2,000,000 PER OCCURRENCE/CLAIM	
NO		MEDICAL MALPRACTICE	$1,000,000 PER OCCURRENCE/CLAIM	
YES		MEDICAL PROFESSIONAL LIABILITY	$5,000,000 PER OCCURRENCE/CLAIM	
NO	11.	MISCELLANEOUS E & O	$500,000 PER OCCURRENCE/CLAIM	
NO	12.	MOTOR CARRIER ACT ENDORSEMENT	$1,000,000 BI/PD EACH OCCURRENCE UNINSURED MOTORIST (MCS-90)	
NO	13.	MOTOR CARGO INSURANCE		
NO	14.	GARAGE LIABILITY	$1,000,000 BODILY INJURY, PROPERTY DAMAGE PER OCCURRENCE	
NO	15.	GARAGEKEEPER'S LIABILITY	$500,000 COMPREHENSIVE; $500,000 COLLISION	
NO	16.	INLAND MARINE BAILEE'S INSURANCE	$	
NO	17.	DISHONESTY BOND	$	
NO	18.	BUILDERS RISK	PROVIDE COVERAGE IN THE FULL AMOUNT OF THE CONTRACT UNLESS PROVIDED BY OWNER.	
NO	19.	USL&H	FEDERAL STATUTORY LIMITS	

20. **CARRIER RATING SHALL BE BEST'S RATING OF A-V OR BETTER OR ITS EQUIVALENT.**

21. **THE COUNTY SHALL BE NAMED AS AN ADDITIONAL NAMED INSURED ON ALL POLICIES EXCEPT WORKERS' COMPENSATION AND AUTO.**

22. **CERTIFICATE OF INSURANCE SHALL SHOW THE PROPOSAL NUMBER AND TITLE.**

23. **OTHER INSURANCE REQUIRED** _____

INSURANCE AGENT'S STATEMENT AND CERTIFICATION: I HAVE REVIEWED THE ABOVE REQUIREMENTS WITH THE PROPOSER NAMED BELOW AND HAVE ADVISED THE PROPOSER OF REQUIRED COVERAGE NOT PROVIDED THROUGH THIS AGENCY.

AGENCY NAME: _____ **AUTHORIZING SIGNATURE:** _____

PROPOSER'S STATEMENT AND CERTIFICATION: IF AWARDED THE CONTRACT, I WILL COMPLY WITH THE CONTRACT INSURANCE REQUIREMENTS.

PROPOSER NAME: _____ **AUTHORIZING SIGNATURE:** _____

ATTACHMENT B
KNOX COUNTY PROCUREMENT DIVISION
IRAN DIVESTMENT ACT/NO BOYCOTT OF ISRAEL

By submission of a response to this solicitation, each proposer and each person signing on behalf of any proposer certifies, and in the case of a joint response each party thereto certifies as to its own organization, under penalty of perjury, that to the best of its knowledge and belief that each proposer is not on the list created pursuant to Tennessee Code Annotated § 12-12-106.

Authorizing Signature:

_____
(sign in blue ink)

Title: _____ Date: _____

Pursuant to Tennessee Code Annotated Title 12, Chapter 4, Part 1, by submission of a response to this solicitation, each proposer and each person signing on behalf of any proposer certifies, and in the case of a joint response each party thereto certifies as to its own organization, under penalty of perjury, that to the best of its knowledge and belief that each proposer is not currently engaged in, and will not for the duration of the contract engage in, a boycott of Israel.

Authorizing Signature:

_____
(sign in blue ink)

Title: _____ Date:_____

ATTACHMENT C
NON-COLLUSION AFFIDAVIT

STATE OF

COUNTY OF

_____, being first duly sworn, deposes and says that:

1. He/She is _____ of _____, the Proposer that has submitted the attached Proposal;

2. He/She is fully informed respecting the preparation and contents of the attached Proposal and of all pertinent circumstances respecting such Proposal;

3. Such Proposal is genuine and is not a collusive or sham Proposal;

4. Neither the said Proposer nor any of its officers, partners, owners, agents, representatives, employees or parties in interest, including this affiant, has in any way colluded, conspired, connived, or agreed, directly or indirectly with any other Proposer, firm or person to submit a collusive or sham Proposal in connection with the Contract for which the attached Proposal has been submitted or to refrain from bidding in connection with such Contract, or has in any manner, directly or indirectly, sought by agreement or collusion or communication or conference with any other bidder, firm or person to fix the price or prices in the attached Proposal or of any other proposer, or to secure through any other proposer, or to fix any overhead, profit or cost element of the proposal price or the proposal price of any other proposer, or to secure through any collusion, conspiracy, connivance or unlawful agreement any advantage against Knox County, TN or any person interested in the proposed Contract; and

5. The price or prices quoted in the attached Proposal are fair and proper and are not tainted by a collusion, conspiracy, connivance or unlawful agreement on the part of the Proposer or any of its agents, representatives, owners, employees, or parties in interest, including this affiant.

(Signed) _____

(Title) _____

Subscribed and sworn to before me

this _____day of _____,2021

_____
(Signature)

My commission expires _____

KNOX COUNTY
TENNESSEE

INFORMATION SECURITY MANAGEMENT POLICY

ZACK WEBB (Feb 23, 2021 11:37 EST)

ZACK WEBB

CHIEF TECHNOLOGY OFFICER

Table of Contents

Introduction

Information Technology (IT) solutions are driven by the demands of our daily business activities at Knox County. The ability to procure efficient communication, IT resources, and technologies that support Knox County's business processes is a foundational component of a successful IT program.

Organizations often take risks in order to meet those time-sensitive business requirements, sometimes bypassing existing processes to meet the demands of customers whom they serve. As we continue to expand our use of cloud technologies, it is imperative that Knox County Information Technology (KCIT) continues to demonstrate that our data is hosted, processed, and stored securely. Information security is not an absolute and cannot absolutely guarantee the security of the information that it handles. This policy is an effort to strive to maintain a reasonable, continuous process for implementing, reviewing, and improving data security.

The main purpose of this living document, the Knox County Information Technology Security Policy, herein thereafter referred to as the "Policy", is to define information security policies for individuals that access any assets controlled, leased, owned, or otherwise utilized by Knox County, herein thereafter referred to as, the "County". Our purview specifically excludes Knox County Libraries, Schools, & Sheriff networks and workstations, with the exception of those Knox County Library, School, and Sheriff users that are issued credentials by KCIT in order to access certain applications and resources. The goal of the Policy is to maintain confidentiality, continuity, integrity, and availability of information, information technology, and critical operation processes in such a manner that the County's legal, regulatory, and ethical responsibilities to its citizens are upheld to the highest of standards. The Policy defines the acceptable use and management of internal and remote systems, services, information, technical controls, and procedures that govern the design, acquisition, implementation, administration, and use of the County's system that assist in mitigating risks due to evolving cyber threats and vulnerabilities.

The Policy defines the minimum-security requirements for the protection of KCIT assets, including the managerial, operational, and technical protection requirements and controls to protect the integrity, continuity, confidentiality, and availability of the County's IT assets as well as compliance with all applicable federal, state, and local laws, policies, and regulations (e.g. HIPAA, HITECH, PCI-DSS, PII, PHI, and other specific privacy regulations currently in effect, as amended, or established later). The Policy will abide by the guidelines established by the National Institute of Standards and Technology (NIST) and any other existing and future implementations of technology, as business needs, and funding allow.

Purpose

The purpose of this policy document is intended to protect any and all information and information systems within the County under KCIT's purview. Information systems consist of all IT systems and critical infrastructure to include computers, communication equipment fixed or mobile, software, systems, applications, databases, internet access, the data and information contained or passing through them, and activities and individual behavior involving the use or management of the systems and information. The intent is to cover all actions and procedures implemented to govern the design,

construction, operation, and preservation of the creation, collection, recording, processing, storing, retrieval, presentation, and transmission of information.

Scope

The Policy applies to:

- All County agencies, departments, employees, volunteers, service providers, vendors, contractors, and commercial entities (referred to as 'users' throughout this and other KCIT policies and procedures), that develop, implement, administer or use Knox County information and communication systems, data and information.
- All audio and video streaming and content, use of any web-based applications, including the use of social media, the County's web addresses (URLs) and image, wireless and remote access into the County's technology environment from anywhere, cloud services, and any other external resources hosted by a third-party, such as a vendor, on behalf of the County are incorporated into the scope of the Policy.
- All existing and future implementations of information systems, communications, other technology, and the Internet at Knox County or in use interoperability capabilities with partner organizations.

Exceptions

Exceptions to the Policy may be requested. Any exceptions to any of the security policies outlined in this, or any other security policy or procedure released on behalf of KCIT, will be reviewed, evaluated, and processed by a member of the Chief Technology Officer's (CTO) staff.

An Information Security Policy Exception/Waiver Request Form shall be prepared by the Department, signed by the elected official or Director of the Department, and submitted for review by the CTO, IT Compliance Officer (ITCO), Cyber Security Manager (CSM) and/or other members of the IT staff, as deemed appropriate. Certain exception requests may require escalation to Knox County's Law Department whose responsibilities include e-Government and HIPAA functions for determination. Periodic reviews for all granted exceptions will be conducted by the ITCO and reviewed by the CTO or Law Department to verify that the original business need is still valid, and the risk level is still acceptable.

Review

Review of this document takes place within KCIT and will occur on an annual basis, at a minimum. Document review can also be requested by submitting a request to the CTO by completing the KCIT Security Policy Document Review Request Form.

Compliance

Objective: **To avoid breaches of legal, statutory, regulatory, or contractual obligations related to information security or any security requirements.**

The Policy shall serve as an adequacy standard for information security safeguards and shall form the basis on which information security audits and reviews will be conducted. All activity from the County's IT environments and on County resources are subject to monitoring by authorized staff or designated entities.

Identification of Applicable Legislation and Contractual Requirements

All relevant legislative, statutory, regulatory, contractual, requirements, and the County's approach to meet these requirements should be explicitly identified, documented, and kept current for each information system, each department, and each entity that stores, processes, or transmits data on behalf of the County. This includes, but is not limited to, Criminal Justice Information Services (CJIS), Health Insurance Portability and Accountability Act (HIPAA), Federal Information Security Modernization Act (FISMA), Payment Card Industry Data Security Standard (PCI DSS), Health Information Technology for the Economy and Clinical Health Act (HITECH), Tennessee Annotated Code, as amended, and the Tennessee Personal and Commercial Computer Act of 2003, as amended.

Privacy and Protection of Personally Identifiable Information

The privacy and protection of personally identifiable information (PII) should be protected as required by relevant federal or state statute or regulation. The overall privacy of information are concerns both for individuals whose personal information is at stake and for departments and agencies that may be liable or have their reputations damaged should PII be inappropriately accessed, used, or disclosed.

Information Security Policies

***Objective*: To provide management direction and support for information security in accordance with Knox County requirements and relevant county, state, and federal statutes, and regulations for the County's computing environments.**

Information Security Requirements and Guidelines

KCIT will initiate, control, and communicate an enterprise information security architecture that includes, but is not limited to, a policy framework, an organizational and communication framework, and a security technology framework.

Security Assessment and Authorization

The CTO shall develop formal and documented security assessment and authorization procedures and strategies that address purpose, scope, roles and responsibilities, management commitment, coordination among agencies and departments, and operations and technical controls to ensure compliance consistent with County policy, and applicable local, state, and federal laws, directives, operational policies, regulations, standards, and guidance.

The CSM and ITCO shall annually review security assessment policies, procedures, and strategies and determine the effectiveness of existing security controls and team roles and responsibilities. The ITCO

shall also produce analytical reports that detail the results of security assessments and implement plans of action to improve information security controls, as funding and budget allow. KCIT may employ an independent assessment team to test and review security controls to ensure compliance consistent with local, state, and federal laws, directives, policies, regulations, standards, and guidance.

County leadership shall determine personnel authorized to determine the acceptable levels of risk to County operations and information assets to guide the implementation of appropriate security controls. County leadership shall designate approval authorities responsible and accountable for exercising due care in assessing the security risks associated with Knox County information and systems and due diligence that the information security program and measures are implemented accordingly.

Department leadership must formally authorize connections from County information systems to external information systems through interconnection security agreements such as Memoranda of Understandings, Service Level Agreements, Firewall Rules Requests, Exceptions to Policy/Waivers, etc. Requests shall include details specific to each connection including the system or data source being connected to, the interface characteristics, security requirements, and type of information transmitted. Interconnections shall be monitored to verify enforcement of security use, policy, controls, and requirements.

The ITCO and/or the CSM shall implement a continuous security program that allows County agencies to maintain security baselines adaptive to evolving threats, vulnerabilities, and technologies yet remain in alignment with County missions, goals, and values.

Operations Security

***Objective*: To protect critical County information resource assets, including hardware, software, and data from unauthorized use, misuse, or destruction and to maintain correct and proper operations.**

Documented Operating Procedures

KCIT and vendors or outsourced employees acting on behalf of the County should identify, document, and maintain standard security operating procedures and configurations for their respective operating environments and make sure the documentation is available to all users who need it.

Awareness and Training

An information security awareness and training program shall be incorporated as part of the County's training and education programs for all users in order to educate the user community in the issues related to vulnerabilities and cyber-security breach risks associated with information technology, the importance, and methods of protecting County information, and information systems. Security awareness shall be continually emphasized, reinforced, updated, and validated.

KCIT shall develop and maintain a communications process for notifying users of new information system security-related issues and concerns specific to the County and of general interest.

Users shall receive security awareness training and sign an acknowledgment indicating they have read and agree to adhere to KCIT information security policies. Records or certifications indicating the completion of security awareness training shall be retained for County users.

Configuration and Change Management

IT systems shall be designed, configured, hardened, and maintained according to County System Hardening Standards to adequately safeguard County information to the extent possible or feasible. Baseline configurations and configuration deviations of the County's information systems, network devices, and communications infrastructure shall be documented, reviewed, and updated. General requirements include, but are not limited to, installing operating systems from KCIT approved sources and media, applying vendor patches, removing, or disabling unnecessary software and services, enabling audit logging and other security protections, and changing the passwords and usernames of default accounts. System owners are prohibited from making unauthorized changes to approved configurations without consultation and approval of the Infrastructure Director and CTO.

System Administrators shall analyze hardware and software for flaws, weaknesses, incompatibility, and other security or functionality impacts and vulnerabilities in a test environment prior to implementation into the production environment, when possible. Security functions shall be reviewed and verified after changes to systems have been implemented to verify the functions and features are implemented correctly, operating as intended, and producing the desired result.

Changes to information processing facilities and systems should be controlled and monitored for security compliance. Formal management responsibilities and procedures should exist to assist in the satisfactory control or all changes to equipment, software, applications, configurations, and/or procedures that affect KCIT operation environment. All written documentation generated by the change control policies and procedures should be retained as evidence of compliance.

Change control procedures should include authorization, risk assessment, logging, auditability, and rollback procedures.

Capacity Management

The use of KCIT resources should be monitored and tuned so that projections of future capacity requirements can be made.

Separation of Development, Testing, and Operational Environments

Development and testing environments should be segregated from production environments in order to reduce the risks of unauthorized access or changes to the production environment. Data classified as restricted must be protected from unauthorized disclosure, use, modification, or destruction and should not be used in development or test environments.

Protection from Malware

Objective: **Prevent the automated propagation of malicious code and contamination of environments attached to the KCIT network.**

Malicious Software Control

All computing platforms that are attached to the County's enterprise technology infrastructure or operated on behalf of the County should be protected from intentional or unintentional exposure to malicious software. Malicious software includes, but is not limited to, software viruses, worms, Trojan horses, logic bombs, and rootkits. Compromised systems should be removed from the operational environment. All computing platforms that are attached to the County's enterprise technology infrastructure will participate in the County's antivirus program if antivirus signatures are available for the computing platforms. KCIT reserves the right to seize any compromised system for forensic analysis.

Backup

Objective: **To prevent loss of data and to attain data availability.**

Data Backup

Backup copies of data, software, and system images should be taken and tested regularly in accordance with the established procedures. A copy of the backup data should be stored off-site according to applicable regulatory requirements and County guidelines. Results of restore tests should be furnished to data owners with recommendations for any remedial steps found. Data owners should approve any remedial plans and timelines for implementing those remediation steps within a reasonable period, not to exceed three months. Following remediation, the restore testing should be repeated and results documented to substantiate that those steps mitigated all identified issues.

Logging and Monitoring

Objective: **To record events and generate evidence.**

Event Logging

All systems should be configured to support security event logging, user activity recording, exceptions, faults, and information security events. System administrators should monitor and report inappropriate access to the Infrastructure Director and the CTO. Critical systems should be configured to support automated logging to a facility that protects the integrity of the logs. Logging levels and monitor elements will be configured in accordance with federal and state statute and regulatory requirements.

Availability and Performance Monitoring

Critical systems should be configured to support County approved automated monitoring of system availability and performance.

Protection of Log Information

Logging facilities and log information should be protected against tampering and unauthorized access.

Administrator and Logs

System Administrator activities should be logged, protected, and regularly reviewed.

Clock Synchronization

Approved KCIT managed enterprise network time servers should be the only County devices permitted to synchronize with external time services. All County provided or managed systems will synchronize time with approved KCIT managed enterprise network time servers. All non-County provided or managed systems storing, processing, or transmitting County data should be synchronized to County approved time synchronization services.

Control of Operational Software

Objective: **To protect the integrity of operational systems.**

Installation of Software on Operational Systems

Only software that has been licensed and approved as County standard software/product or that has been approved as an exception through the County's architecture standards approval process should be installed on devices covered by the software's license agreement.

Patch Management

All applications and processing devices that are attached to the County's enterprise technology infrastructure will have critical security related application, operating system, and/or security-related patches for supported operating systems made available by the software or hardware vendor applied when applied within 90 calendar days or sooner, if any acceptable date can be agreed upon by all affected parties. Emergency patches and updates will be applied as soon as possible following successful validation and testing.

Patch Schedule

KCIT will generally follow the below schedule for patches, unless deemed otherwise.

- 7 days for critical patches addressing known exploits
- 14 days for high patches addressing known exploits
- 30 days for critical patches
- 60 days for high patches

Software Maintenance

Servers and workstation computer devices should have defined maintenance windows within every 90 days.

Applications should have established review and maintenance cycles for software updates.

Access Control

Objective: **To limit access to information and information processing facilities.**

Access Control Policy

All access rules and requirements to access KCIT resources should be developed, documented, maintained, and audited by KCIT. Access to the County's IT resources will be granted consistent with the concept of least privilege. All information processing systems owned by or operated on behalf of the County should have an appropriate role-based access control system that confirms only legitimate users and/or systems have access to IT resources that are explicitly authorized to use.

Access to Networks and Network Services

All access and connectivity to the County's enterprise network or networks operated on behalf of the County should be granted consistent with the concept of least privilege. Users will only be provided with access to the network and network resources that they have been specifically authorized to use.

Remote Access

All users who are accessing the County's internal network should access those resources through a County approved Virtual Private Network (VPN) solution. All users who access County data on networks operated on behalf of the County should use secure connection methods and are required to sign the Acceptance Use Policy and End User Agreement.

Information Security Roles and Responsibilities

All information security responsibilities should be defined and assigned by the access granting authority within KCIT, most commonly the system administrators.

Segregation of Duties

Where appropriate, conflicting duties and areas of responsibility should be segregated and assigned to different individuals to reduce opportunities for unauthorized or unintentional modification or misuse of the County's assets.

User Access Management

Objective: **To authenticate authorized user access and to prevent unauthorized access to systems and services.**

User Registration and De-Registration

A formal user registration and de-registration process will be implemented to enable proper assignment of access rights and to adjust those rights as the user's role changes. Prior to any access, the user must complete, sign, and return the KCIT Acceptable Use Policy and End User Agreement.

User Access Provisioning

User access to IT resources should be authorized and provisioned according to the Department's employee provisioning process.

User Account Naming

All County user accounts will follow a County approved standardized naming convention.

Management of Privileged Access Rights

Users should have the least privileges required to perform their roles as identified and approved by their management. The allocation and use of privileged access rights should be restricted and controlled.

Management of Secret Authorization of Information Users

The allocation of secret authentication information should be controlled through a formal management process.

Review of User Access Rights

A user's access rights should be reviewed, validated, and updated for appropriate access provided by a user's supervisor on a regular basis or whenever the user's access requirements change (e.g. hire, promotion, demotion, and transfer within and between departments). KCIT is not responsible for determining appropriate user access rights. However, KCIT will provide departments with audit reports, upon request.

Removal or Adjustment of Access Rights

All access rights for employees, elected officials, and external entities to information and information processing facilities should be revoked upon termination of their employment, contract, agreement, or change of department by the close of business on the user's last day working or within 24 hours of notification of the user's death, determination of job abandonment, or retroactive notification of resignation or retirement.

In the event the user will be returning or transferring to another role in which they will need access to the County's resources, the user's profile will be suspended in lieu of termination and the user's access rights will need to be reviewed prior to reinstatement.

Procedures for emergency removal of access rights should be in place.

User Responsibilities

Objective: **To make users accountable for safeguarding their authentication information.**

Use of Secret Authentication Information

Users should follow County guidelines and requirements in the use of secret authentication information.

System and Application Access Control

Objective: **To prevent unauthorized access to systems and applications.**

Information Access Restriction

Access to information and application system functions should be restricted in accordance with the defined access control guidelines. KCIT reserves the right to deny access to any networked information, systems, applications, or internal resources for any devices not owned by the County.

Secure Log-on Procedures

Where required by access control guidelines, access to systems and applications should be controlled by a secure log-on procedure. At a minimum, user access to protected KCIT resources requires that the utilization of User Identification (User ID) and password that uniquely identifies the user. Sharing access credentials intended to authenticate and authorize a single user between any two or more individuals is prohibited.

System Administrator Access

All System Administrators or users with elevated privileges using administrative tools or protocols to access servers located in County managed data processing facilities or facilities operated on behalf of the County must use a multifactor VPN solution to obtain access.

Log-on Banner

All workstations owned and operated by or on behalf of the County must display the County approved logon banner before the user is able to log in.

Service Account Use

Service Accounts should be unique to each application and/or system and should only be used to authenticate systems and/or applications to specific services.

System/Application Account Use

System/application accounts are created upon installation of an application and may have a predetermined User ID. Privileged user access to system accounts must be approved and documented. A system/application account differs from a service account in that individuals may know the password

to the system/application account. This account must be elevated from a lesser account. An example of this type of account is the default administrative account required by the application.

System Administrator Account Use

System Administrator accounts have elevated privileges and should only be used when elevated privileges are required. Administrative accounts are used to administer operating systems and applications.

Password Requirements

All users accessing Knox County internal resources are required to adhere to the requirements and guidelines set forth in the Knox County Password Requirements & Guidelines document. When accessing applications, users must adhere to the password requirements of the application that will be accessed.

Password Management System

Password Management Systems should be interactive and should ensure quality passwords. Passwords and passcodes must be provided to KCIT upon request.

Use of Privileged Utility Programs

The use of utility programs that might be capable of overriding system and application controls should be restricted and tightly controlled.

Access Control to Program Source Code

Access to program source code should be restricted to authorized users.

Default Configurations

All applications and processing devices that are attached the County's enterprise technology infrastructure should be deployed with modified configurations for, but not limited to, default accounts, and/or installation paths to minimize the use of default settings to gain unauthorized use, modification, or destruction.

Asset Management

Objective: **To identify organizational assets and define appropriate protection responsibilities.**

Inventory of Assets

An inventory of information system assets, components, software, and services in KCIT's custody and control shall be maintained and periodically reassessed. Due to the varying values of equipment under KCIT's purview, an agreed-upon threshold between the CTO and Knox County Finance Department will determine the minimum value of an asset that is required to be included in KCIT inventory.

Ownership of Assets

All information resource assets listed in the asset inventory should have an assigned owner or entity who will ensure the assets are protected in a manner consistent with their value, sensitivity, and criticality to the business and operation of the County's government and those it serves or as specified by any superseding county, state, or federal statute or regulation.

Acceptable Use of Assets

Rules for the acceptable use of information and assets associated with information and information processing facilities should be identified, documented, implemented, and communicated to the users who have access to those assets.

Users are expected to treat their assets with care and respect. Placing stickers, writing, or drawing on, engraving, or otherwise defacing any device(s) and/or case(s) is prohibited, unless authorized by KCIT, and may result in loss of the privilege of utilizing a County-owned asset.

Return of Assets

All users of KCIT assets must return all County assets in their possession upon termination of their need to no longer access KCIT information or information systems. All assets must be returned unlocked. In the event an asset is returned, and it is locked, Knox County reserves the right to withhold the user's last paycheck until the user unlocks all assets that were in the user's custody.

Asset Identification

All KCIT workstations will be named in accordance with an approved standardized naming convention. Those identification numbers shall be affixed in obvious locations when possible.

Data Classification

Objective: **To confirm the data used and managed by the County receives an appropriate level of protection commensurate with the value, importance, and criticality of the data to the County.**

Classification of Data

Data assets owned and/or managed by the County should be classified according to the definition of "Personal Information" or "Confidential Records" as specified by applicable state and/or federal statute or regulations to indicate the need, priorities, and degree of protection it will receive. At a minimum, data will be classified as Public, Internal, or Restricted.

Labeling of Data

An appropriate set of procedures for labeling data assets owned and/or managed by the County should be developed and implemented in accordance with the County's data classification scheme.

Handling and Use of Data

Procedures for handling data assets should be developed and implemented in accordance with the data classification scheme adopted by the County.

Public Data Classification and Control

Data classified as public should be protected from unauthorized modification or destruction.

Restricted Data Classification

Data classified as restricted must be protected from unauthorized disclosure, use, modification, or destruction and cannot be used in development or test environments, or publicly disclosed. Controls should be applied to data in a manner consistent with its value, sensitivity, and criticality to the business and operation of the County. Data classified as restricted must be encrypted at rest and during transmission in accordance with applicable state or federal statute or regulatory requirements.

Restricted Data on Personally Owned Devices

Restricted data, specifically PHI and PII, should not be stored on, or accessed using personally owned devices, including mobile devices (cell phone, tablet, etc.), unless an Information Security Policy Exception/Waiver Request Form has been completed, submitted, and approved.

Restricted Electronic Messages Classification and Control

Email sent from the County's domain out through the public Internet must be encrypted if it contains restricted information in the body or attachment. Restricted information should not be placed into the subject line of the message.

Payment Card Information Classification and Control

Payment card information must be considered restricted when an individual's first name or first initial and last name are present in combination with account number, credit or debit card numbers, required security code, access code, or password that would permit access to an individual's financial account.

The Payment Card Industry – Data Security Standards (PCI DSS) comprise a minimum set of requirements for protecting cardholder data and may be enhanced by additional controls and practices to further mitigate risks, as well as local, regional, and sector statutes and regulations. Additionally, legislation or regulatory requirements may require specific protection of PII and/or other data elements (for example, cardholder name).

All payment card information stored and processed by the County or transmitted over County networks must be in compliance with the PCI-DSS. Storage of the full Primary Account Number (PAN) on County systems is prohibited.

All purchased (off the shelf) applications used to process payment card information must be compliant with the Payment Application Data Security Standard (PA-DSS).

Media Handling

Objective: **To prevent unauthorized disclosure, modification, removal, or destruction of data stored on media.**

Management of Removable Media

Procedures should be implemented for the management of removable media in accordance with the classification scheme adopted by KCIT.

Repair of Removable Media

Removable media should be sanitized prior to removing it from the County facilities for maintenance and repair.

Disposal of Removable Media

Removable media should be disposed of securely when no longer required, using KCIT approved procedures.

Physical Transfer of Removable Media

Removable media containing restricted data must be protected against unauthorized access, misuse, or corruption during transport.

Workstation Computing

Objective: **To prevent unauthorized disclosure, modification, removal, or destruction of data stored on user assigned processing devices.**

County Provided Workstation Computing Platforms

Workstation computing platforms, including laptops, should be physically protected against theft when left unattended. Workstation computing platforms should not store restricted data assets where it is not absolutely necessary to perform the specific job-related duties. Storage of restricted data assets on a workstation computing platform should have approval from the asset custodian for such storage. Restricted data assets that have been authorized to be stored on the local workstation should be encrypted while stored on the workstation computing platform.

Workstation Platform Reassignment

All workstation computing platforms, including all external storage devices, should be sanitized prior to being re-issued or re-purposed to another user.

Workstation Platform Disposal

Hard drives in workstation computing platforms, including all mobile storage devices and phones, should be sanitized using approved sanitization procedures, or destroyed prior to transfer or surplus of a processing device to an external entity.

Cloud & Hosting Services

Anyone acting on behalf of the County who wishes to use cloud or hosting services for County business must seek KCIT guidance and approval for cloud solutions prior to enabling cloud services. This is imperative due to the higher risk of security concerns and threats associated with cloud computing.

KCIT will perform conformity assessment activities that may include, but are not limited to, the review and approval of service level agreements, terms and conditions, privacy policies, monitoring services, accessibility, standards mapping, standardization gaps, and retention policies.

Physical and Environmental Security

Objective: **To prevent unauthorized physical access, damage, and interference to the County's information and information processing facilities.**

Physical Security Perimeter

All enterprise data processing facilities that process or store data classified or restricted should have multiple layers of physical security. Each layer should be independent and separate of the preceding and/or following layer(s).

All other processing facilities should have, at a minimum, a single security perimeter protecting it from unauthorized access, damage and/or interference.

Physical Entry Controls

Secure areas should be protected by appropriate entry controls to restrict access only to authorized personnel.

Securing Offices, Rooms, and Facilities

Physical security for offices, rooms, and facilities should be designed and applied commensurate with the classification and value of the data being handled or processed.

Protecting against External and Environmental Threats

Physical protection against natural disasters, malicious attacks, or accidents should be considered and incorporated in facility design, construction, and placement.

Working in Secure Areas

Procedures for working in secure areas should be created and implemented.

Delivery and Loading Areas

Access points such as delivery and loading areas and other points where unauthorized persons could enter the premises should be controlled, and if possible, isolated from information processing facilities.

Equipment

Objective: **To prevent loss, damage, theft, compromise of assets, or interruption to County operations.**

Equipment Siting and Protection

Equipment should be located in secured areas or protected to reduce the risks from environmental threats or hazards, and to reduce the opportunities for unauthorized access. Equipment located in areas where Knox County is unable to maintain a secure perimeter should be locked in a secured manner with access controlled by Knox County. Secured cabinets or facilities should support further segregation within KCIT organization based on role and responsibility.

Supporting Utilities

Infrastructure and related computing equipment should be protected from power failures and other disruptions by failures in supporting utilities.

Cabling Security

Power and telecommunications cable carrying data or supporting information services should be protected from interception, interference, or damage.

Equipment Maintenance

Equipment should be correctly maintained to ensure its continued availability and integrity.

Removal of Assets

All equipment, software, or information that is a part of KCIT operational systems or processes should not be taken off-site without the prior authorization from executive management or a designated representative and should be removed according to documented KCIT equipment transfer procedures.

Security of Equipment and Assets Off-Premises

Security should be applied to off-site assets, taking into account the different risks of working outside the County's premises.

Secure Disposal or Reuse of Data Processing Equipment

All data processing equipment including storage devices subject to transfer or reuse should be sanitized with KCIT's media reuse procedure or superseding state or federal requirements. Data processing equipment assets that are not subject to transfer or reuse should be destroyed in accordance with KCIT's media disposal procedures or in accordance with superseding state or federal requirements.

Unattended User Equipment

Users should ensure that unattended data processing equipment has appropriate protection.

Session Time Outs

All systems and devices owned and operated by or on behalf of Knox County should be configured to clear and lock the screen or log the user off the system after a defined period of inactivity. Sessions will be configured to time out after a minimum of 15 minutes of activity.

Clear Desk and Clear Screen Policy

All data classified as restricted must be stored in a locked cabinet or room when unattended. All data processing equipment that provides access to Information Processing Systems will be configured so that a screensaver, with password protection engaged, or other lock-down mechanisms that prevent unauthorized viewing of screen information or unauthorized access to the system will automatically be implemented if the system has been left unattended. Maximum inactivity interval for engaging screensaver or other lockdown mechanisms is 15 minutes.

All restricted computing platforms residing in non-secured facilities with attached displays should be oriented away from direct line of sight from unauthorized viewers.

Network Connectivity Security

Objective: **To protect the County's assets that are accessible by suppliers and vendors.**

Network Controls

Networks should be managed and controlled to protect information in systems and applications.

Security of Network Services

Security mechanisms, service levels, and management requirements of all network services should be identified and included in network services agreements, whether these services are provided in-house or outsourced.

Segregation in Networks

All enterprise network architectures operated by, or on behalf of, Knox County should be designed to support, at a minimum, separate public, "demilitarized" and private security zones based on role, risk, and sensitivity. Bridging between separate security zones is strictly prohibited. All access between

separate security zones should be controlled by a security mechanism configured to deny all access by default unless explicitly authorized and approved by KCIT.

Information Transfer

Objective: **To maintain the security of information transferred within network infrastructures managed by and on behalf of Knox County and with any external entity.**

Information Transfer Policies and Procedures

Formal transfer procedures, guidelines, and controls should be in place to protect the transfer of information through the use of all types of communication facilities.

Agreements on Data Transfer Policies

Agreements should address the secure transfer of business information between the County and external parties.

Electronic Messaging

Data involved in electronic messaging should be appropriately protected.

Internal Electronic Messages Control

Email and instant messages internal to the County's domain containing restricted data should be encrypted during transmission. Restricted information should not be placed into the subject line of email or as any part of instant message.

External Electronic Messages Control

Email sent through the public Internet must be encrypted if it contains restricted information in the body or attachment of the email. Restricted information should not be placed into the subject line of the message.

Electronic Messaging Management

All electronic messages created, sent, or received in conjunction with the transaction of official business should use the County's approved gateway(s) to communicate via the Internet.

Confidentiality or Non-Disclosure Agreements

When exchanging or sharing information classified as restricted with external parties that are not already bound by a contract confidentiality clause or a non-disclosure agreement, one should be established between the owner of the data and the external party.

Note: Departments should work with Knox County legal counsel to ensure proper language is used.

Mobile Device Security Policy

Objective: **To extend the County's security posture to the mobile workforce.**

Mobile Device Policy

All Knox County owned mobile devices that connect to KCIT managed data or infrastructure should be managed by the County's enterprise mobile device management solution or the County's enterprise configuration manager, as funding allows, and should comply with appropriate mobile device usage policies as required by state or federal statute or regulation.

Alternate Work Space

Alternate Work Space (AWS) users should comply with the appropriate AWS policies as required by state or federal statute, regulation, or state, county, or department policy, procedures and/or guidelines.

External Party Security

Objective: **To protect the County's assets that are accessed, processed, communicated to, or managed by external parties, suppliers, or vendors. This includes any external party who has access to physical data processing facilities, logical access to County data processing systems via local or remote access, or access via another external party into the County's data processing facilities.**

Information Security Policy for External Party Relationships

Information and physical security requirements for mitigating the risks associated with supplier or vendor access to the County's assets should be agreed upon in writing with the external party. All external parties must agree in writing to comply with all applicable information security policies, third party connectivity agreements, executive orders, standards, controls, and regulations.

Identification of Risk

Risk involving external parties should be identified and proper controls implemented prior to the granting of access to any County information, information technology asset or information processing facilities.

Addressing Security within External Party Agreements

All relevant information security requirements should be established and agreed upon with each supplier or vendor that may access, process, store communicate any County data as well as access, process, store, communicate, or provide IT infrastructure components for the County's processing systems or infrastructure.

Reporting of Security Incidents

External Party Agreements will require external parties to report perceived security incidents that may impact the confidentiality, integrity, or availability of County data immediately.

Subcontractor Requirements

Primary external parties should require their subcontractors to abide by the County's policies and security requirements, if applicable.

Addressing Security for Access to Citizen Data

Risk involving external party access to citizen data should be identified and proper controls implemented prior to the granting of access to any County citizen data. Appropriate controls should be agreed upon, documented in external party agreements, and implemented prior to the granting of access to any citizen data.

System Acquisition, Development, and Maintenance

Objective: **To verify that information security is an integral part of information systems through its life cycle. This includes application infrastructure, vendor applications, inhouse development, and user-developed applications and information systems which provide services over public networks or the County's internal network.**

Security Requirements of Information Systems

Security requirements should be identified and documented as part of the overall business case for new information systems and for enhancement to existing information systems and should be included early and continuously throughout the lifecycle of the application, including, but not limited to the conception, design, development, testing, implementation, maintenance, and disposal phases.

Securing Application Services on Public Networks

Information involved in application services passing over public networks should be protected from fraudulent activity and unauthorized disclosure or modification.

Protecting Application Services Transactions

Information involved in application service transactions should be protected to prevent incomplete transmission, misrouting, unauthorized message alteration, unauthorized disclosure, unauthorized message duplication or reply.

Information Security in Project Management

Information security should be addressed at project initiation and throughout the lifecycle of the project.

Security in Development and Support Processes

Objective: **To confirm that information security is designed and implemented within the development lifecycle of information systems.**

Security Requirements of Information Systems

Requirements, rules, and guidelines for the development of software and systems should be established and applied to all systems development.

Security in Application Systems Development

Input validation, authentication, and authorization should be included in the design, development, and implementation of applications.

Input and Data Validation

Applications should not pass raw input to other processes including, but not limited to, other applications, web services, application servers, and databases. Non-legacy applications should use parameterized queries or stored procedures, and not dynamic SQL statements, when processing user input.

Output Data Validation

Applications should not echo input back to the user or disclose information about the underlying system through error messages.

Application Authorization

Applications that provide access to restricted information in databases or from network shares should perform user authentication.

Inter-process Message Authentication

Inter-process message authentication should be used to verify that a message originated from a trusted source and that the message has not been altered transmission.

Control of Internal Processing

Security controls should be included to prevent corruption due to processing errors or deliberate acts.

Change Control Procedures

Changes to systems or applications within the development lifecycle should be controlled by the use of formal change control procedures.

Technical Review of Applications after Operating Platform Changes

When operating platforms or applications are changed, business critical applications should be reviewed and tested to verify there is no adverse impact on organizational operations or security.

Restrictions or Changes to Software Packages

Modifications to software packages should be limited to necessary changes, and all changes should be strictly controlled.

Secure System Engineering Principles

Principles for engineering secure systems should be established, documented, maintained, and applied to any information system implementation efforts.

Secure Development Environment

Organizations should establish and appropriately protect secure development environments for system development and integration efforts that cover the entire system development lifecycle.

Outsourced Development

Outsourced system development should be monitored and supervised to ensure the County's policies and practices are followed and to confirm appropriate security controls are in place. This is applicable for KCIT and any other departments within the County that develop applications.

System Security Testing

Testing of security functionality should be carried out during development. Applications should be tested periodically throughout their respective lifecycles, at each major version release, and prior to assigning public IP addresses or being moved or promoted into the production environment.

System Acceptance Testing

Acceptance testing program and related criteria should be established for new information systems, upgrades, and new versions.

Protection of Test Data

Test data should be selected carefully, protected, and controlled.

Business Continuity Management

Objective: **To maintain the availability of critical systems and infrastructure with the continued ability to provide services in the event of a crisis or disaster.**

Planning Information Systems Continuity

KCIT should determine its requirements for the continuity of information management systems in adverse situations, e.g. during a crisis or disaster. County departments are encouraged to communicate the criticality of operation information systems to KCIT and engage in disaster recovery exercises.

Business Impact Analysis

KCIT should perform a Business Impact Analysis (BIA) to identify systems and infrastructure that are critical to County operations and services to citizens, other departments, and agencies, as well as regulatory bodies.

Critical Applications

Systems including Infrastructure components, applications, and security systems identified as critical in the BIA will be recovered in accordance with the BIA and documented system recovery strategy.

Non-Critical Applications

Infrastructure components and applications identified as non-critical in the BIA will be recovered on a best-effort basis. The components and applications listed as non-critical should have an explanation in the BIA justifying their low importance and demonstrating how the loss of their associated functionality will be acceptable during an event or how a manual workaround can be implemented.

Implementing Information Systems Continuity

KCIT should establish, document, implement, and maintain processes, procedures, and controls in disaster recovery plans to make sure the required level of business continuity for all systems during an adverse situation are considered and addressed.

Verify, Review, and Evaluation Information Systems Continuity

KCIT, vendors, and/or contractors who operate on behalf of the County should verify they established and implemented information systems continuity controls at regular intervals in order to ensure that they are valid and effective during adverse situations.

Redundancies

Objective: **To attain availability of information processing facilities.**

Availability of Information Processing Facilities

Information processing facilities should be implemented with redundancy sufficient to meet availability requirements.

Verify, Review, and Evaluate Information Systems Continuity

BIAs and a sample of critical applications should be tested within every 365 days as a part of a scheduled disaster recovery exercise, as a tabletop exercise, or prior to go live exercise.

Information Security Incident Management

Objective: **To create a consistent and effective approach to the management of information security incidents, including communication on security events and weaknesses.**

Responsibilities and Procedures

KCIT will establish a Security Incident Response Team (SIRT). The SIRT will ensure that the County can efficiently and effectively communicate information security incidents to the proper stakeholders and respondents of the County. The SIRT members will be appointed based on their position and capabilities within the organization and their responsibilities communicated clearly.

Reporting Information Security Events

Information security events should be reported through appropriate channels using the Knox County Cyber Incident Response Plan (CIRP).

Data Breach and Disclosure

Anyone that discovered a breach of the information security controls set forth in this document which results in disclosure of unencrypted "personal information" about persons to unauthorized third parties must provide disclosure in accordance with TCA 47-18-2107 or any other applicable state and/or federal statute or regulations).

Reporting Information Security Weakness

Employees, outsourced employees, and any users using the County's information systems and services are required to note and report any observed or suspected information security weaknesses in systems or services to KCIT.

Assessment of and Decision on Information Security Events

Information security events should be assessed, and a determination should be made on whether to classify the event as an incident in accordance with the CIRP.

Response to Information Security Incidents

Information security incidents will be managed in accordance with the documented procedures in the KCIT Incident Response, Alerting, and Communication Plan.

Learning from Information Security Incidents

Knowledge gained from analyzing and resolving information security incidents should be used to reduce the likelihood or impact of future incidents.

Collection of Evidence

The County should define and apply procedures for the identification, collection, acquisition, and preservation of information, which can serve as evidence.

Cryptography

Objective: **To achieve proper and effective use of cryptography to protect the confidentiality and integrity or data owned or managed by or on behalf of the County. Restricted information must be encrypted by the use of valid encryption processes for data at rest and in motion as required by state or federal statute or regulation. This includes but is not limited to sensitive information stored on mobile devices, removable drives, and laptop computers.**

Use of Cryptographic Controls

Cryptographic controls should be based on the classification and criticality of the data. In deciding what strength and type of control to be deployed, both stand-alone and enterprise level encryption solutions should be considered. Attention should be given to regulations, national restrictions (e.g. export controls) that may apply to the use of cryptographic techniques.

Transmission Confidentiality

Information systems should protect the confidentiality of transmitted information. The County will employ mechanisms to recognize changes to information during transmission unless otherwise protected by alternative physical measures.

Cryptographic Module Authentication

Information systems must use mechanisms for authentication to a cryptographic module that meet the requirements of application federal statutes, state statutes, Executive Orders, directives policies, regulations, standards, and guidance for such authentication. The list of cryptographic modules in use will be compared to the list of NIST validated cryptographic modules at least quarterly ensure compliance.

Information systems will obtain, and issue supported public key and Transport Layer Security (TLS) certificates from an approved service provider. This control focuses certificates with visibility external to the internal system operations, for example, application-specific time services. Secure Socket Layer (SSL) protocol must be disabled on all devices.

Key Management

A secured environment should be established to protect the cryptographic keys used to encrypt and decrypt information. Cryptographic key management and establishment will be performed using automated mechanisms with supporting manual procedures. Keys should be security distributed and stored. Access to keys should be restricted only to individuals who have a business need to access them. All access to cryptographic keys requires authorization and should be documented. Compromise of a cryptographic key would cause all information encrypted with that key to be considered unencrypted.

Technical and Vulnerability Management

Objective: **To prevent exploitation and technical vulnerabilities.**

Management of Technical Vulnerabilities

Information about technical vulnerabilities on information systems and supporting infrastructure should be obtained in a timely fashion, evaluated for exposure and risk to the County, and appropriate measures implemented to address the associated risk.

Restrictions on Software Installation

Users should not install software that has not been approved by KCIT and their supervisor.

Information Systems Audit Controls

In order to minimize the impact of audit activities on operational systems, audit requirements and activities involving verification of operational systems should be carefully planned and agreed upon in advance to minimize disruptions to business processes.

Policy Name		Document Reference Number: KCIT.SMP.1
Information Security Management Policy	**Version #**	1
	Signed **Signed**	Zack Webb _____
	Approval Date	February 22, 2021
	Implementation Date	February 22, 2021
	Last Reviewed by County Commission	February 22, 2021