Executive Branch Information Technology
Office of Information Technology Services
2800 SW Topeka Blvd., Building 100
Topeka, KS 66611

Kansas
Office of Information Technology Services

Phone: (785) 296-3463
Fax: (785) 296-1168
oits.info@ks.gov

Jeff Maxon, Interim Chief Information Technology Officer

Laura Kelly, Governor

February 24, 2023

Todd Herman, Director
Procurement and Contracts

Dear Mr. Herman:

The detailed project plan for the University of Kansas Medical Center Security Infrastructure – SIEM project is enclosed. Chris Harper is the primary contact for the project and can be reached at (913) 945-8543. This letter constitutes approval of the detailed project plan pursuant to K.S.A. 75-7209.

KUMC - Security Infrastructure – SIEM is an infrastructure/commercial off-the-shelf software solution to support a technology layer and thus does not fit traditional project monitoring parameters. The project is required to provide quarterly project reporting transmittal pages for the duration of the project. However, we are exempting the project from all other quarterly report requirements contained in ITEC Policy 2500.

This project has a total project cost of $352,501. The quarterly KITO fee for the project will be $123 and will be billed from the start of Execution until receipt of the project's Post Implementation Evaluation Report (PIER).

Respectfully,

DocuSigned by:
Jeremy Pennington
1C6FB0FF67F8497...
Jeremy Pennington, Chief Information Security Officer (CISO)
The University of Kansas Medical Center

DocuSigned by:
Jeff Maxon
670B8750658F441...
Jeff Maxon, Interim CITO
Executive Branch

cc: Kelly O'Brien, CITO, Judicial Branch
Alan Weis, CITO, Legislative Branch
Adam Proffitt, Director of the Budget
James Fisher, KLRD
JCIT Membership
Kelly Johnson, OPC
Brian Reiter, OITS
Chris Harper, KUMC
James Dillon, KUMC
Megan Burton, KSHS
Cole Robison, OITS
Alex Wong, CITA
Sash Smith, OITS
Sara Spinks, KITO

December 6, 2022

Dr. DeAngela Burns-Wallace
Secretary of Administration and Chief Information Technology Officer, Executive Branch
900 SW Jackson Street, Room 751
Landon State Office Building
Topeka, KS 6612-1275

Dear Dr. Burns-Wallace,

This letter is our formal request for approval to implement an information security infrastructure project.

Enclosed, you will find the detailed project plan and supporting documents required for information technology projects.

Upon approval, we will begin implementation.

We look forward to hearing from you soon. Thanks, and very best wishes.

Sincerely,

DocuSigned by:
Jeremy Pennington
1C6FB0FF67F8497...

Jeremy Pennington
Chief Information Security Officer (CISO)
The University of Kansas Medical Center
4330 Shawnee Mission Parkway
Fairway, Kansas 66205

State Entity Checklist for Detailed IT Project Plan

State Entity: KUMC	Included (Y/N) If no, Explain
Project Name: KUMC - Security Infrastructure - SIEM	
Greater than $250,000/ less than $1,000,000 (Y/N): Y	
Greater than $1,000,000 (Y/N): N	
IT Project Plan Documents	
For forms and/or more detailed information on completion of plan, see https://ebit.ks.gov/kito/it-project-oversight/proposed-it-project-plans	
For ITEC Policy and/or more detailed information on approval of IT projects, see ITEC 2400 and 2400A. https://ebit.ks.gov/itec/resources/policies	
Cover Letter Requesting Project Approval	Y
IT Project Request Explanation--DA518	Y
IT Cost Benefit Statement--DA519	Y
Work Breakdown Structure @ 8/80 hr duration/elapsed calendar time level	
Task Name (tasks should be descriptive)	Y
Duration (total duration/elapsed calendar time)	Y
Work (total person/hours of effort for all resources for the task)	
Start	Y
Finish	Y
Dependencies (Predecessors)	Y
Resource Names (assigned to the task)	Y
Milestone	Y
Work Product Identification (Form ITEC PM02-6)	Y
Architectural Statement (ITEC Policy 4010 and 9500) https://ebit.ks.gov/itec/resources/policies	
Listing of products and standards that will be implemented to accomplish the project including a statement of compliance with ITEC Policy.	Y
If different, attach CITA waiver	N/A
Ownership of Software Code and Related Intellectual Property (ITEC Policy 1500) https://ebit.ks.gov/docs/default-source/itec/itec_policy_1500.pdf	
Statement of compliance	Y
If different, attach CITO waiver	N/A
Privacy Statement (Privacy Act 1974, Health Insurance Portability & Accountability Act 1996-HIPAA) https://www.justice.gov/opcl/overview-privacy-act-1974-2015-edition	
https://www.hhs.gov/hipaa/index.html	
1. What information is included	Y
2. Why is it collected	Y
3. How will it be used	Y
4. Exclusion opportunities	Y
5. 1974 Act implementation	Y
6. Other privacy requirements	Y
7. Total privacy cost estimate	Y
Security Statement (ITEC Policy 4210, 7220, 7230, 9500, 7300, 7310) https://ebit.ks.gov/itec/resources/policies	
Statement of compliance regarding security measures, technologies used, compliance with policy & standards	Y
If different, explain	N/A
Accessibility Statement (ITEC Policy 1210) https://ebit.ks.gov/itec/resources/policies/policy-1210	
Confirm the project will comply with ITEC Policy 1210 requirements by attaching a completed Accessibility Conformance Report (ACR) produced using the Voluntary Product Accessibility Template® (VPAT®), version 2.0 or later, for the product(s) procured, provided as a service, or custom-built. If requirements are to be developed as part of project, indicate that VPAT requirements will be included. See VPAT at: https://www.itic.org/policy/accessibility/vpat.	Working with Exabeam to receive VPAT - will forward for review.
If VPAT/ACR indicates compliance on all items, provide statement identifying task number(s) in WBS where verification of overall compliance will occur. For any VPAT/ACR item(s) where full compliance is not indicated, identify task number(s) in WBS where remediation of compliance issues will occur, and the task number(s) that will include verification of overall compliance. **If product is not anticipated to be compliant upon initial implementation, please attach State ADA Coordinator exception.** If accessibility standards do not apply, please provide explanation.	N/A
Attach approval letter from State Director of IT Accessibility.	Waiting for approval
Electronic Record Retention Statement https://www.kshs.org/p/electronic-records/11334 (K.S.A. 45-403 and K.S.A. 45-213 through 45-223)	
1. Identify replaced paper records	Y
2. Identify new business functions	Y
3. Reasons for business functions	Y
4. Records requirements for business function	Y
5. Documents in another system?	Y
6. Public access requirements	Y
7. Access control requirements	Y
8. Identify all records with retention period of ten or more years	Y
9. Estimate three year cost of addressing records identified in No. 8	Y
Attach approval letter from State Archivist.	Y
Risk Identification Summary (Form ITEC PM02-11a)	Y
Risk Assessment Model (RAM) Summary - Detailed Plans	Y
Fiscal Note, if appropriate	
Electronic copy submitted two - four weeks prior to contract award and/or project execution	

INFORMATION TECHNOLOGY PROJECT REQUEST EXPLANATION -- DA 518

1. Project Title:	2. Project Priority	3. Estimated Dates	
KUMC - Security Infrastructure - SIEM	High	**Planning Start:**	5/26/2022
Agency:		**Execution Start:**	1/16/2023
Kansas University Medical Center		**Close-Out End:**	5/19/2023
4. Project Description and Justification:	**Date Submitted:**	12/6/2022	

This proposed project is designed to help KUMC implement the most appropriate hardware and software infrastructure for our requirements. This is an IT infrastructure project that entails implementing a security information and event management (SIEM) information security infrastructure.

The justification for this project is the need for KUMC to upgrade and replace the current SIEM. The SIEM offers real-time monitoring and analysis of events as well as tracking and logging of security data for compliance or auditing purposes. SIEM will help enable KUMC support for security and compliance management requirements. SIEM, broadly speaking, is a security solution that will continue to help KUMC recognize potential security threats and vulnerabilities before they have a chance to disrupt business operations. It surfaces user behavior anomalies and uses artificial intelligence to automate many of the manual processes associated with threat detection and incident response. It will continue to provide KUMC with capability to prevent, monitor, and mitigate high-risk events for KUMC. The ability for KUMC to continue their work in improving lives and communities in Kansas and beyond through innovation in education, research, and health care is the business objective and the primary driver for this project.

Is this an Infrastructure Project? (Y/N)	Y
Will Business Process Modeling be completed during the IT project and business design? (Y/N)	Y
Will national and/or industry data standards be used? (Y/N)	Y
If yes, please specify.	At the national level, relevant National Institue of Standards and Technology (NIST) 800 series and NIST CSF (Cybersecurity Framework) standards will be used where possible. Other federal regulatory standards such as Health Insurance Portability and Accountability Act (HIPAA) will be used, where possible, to define data components within the SIEM solution. Guidance provided by the relevant State of Kansas ITEC policies and industry guidance from Payment Card Industry Data Security Standard (PCI

List any collaboration that has taken place in the planning of the IT Project, and/or will take place during execution of the project. Include tools, methods, and best practices used for providing collaboration, user input, and continued social networking.

Organizational leadership, internal business units, and key partners to KUMC have been or will be consulted for the planning, execution, and deployment of this project. The collaboration has or will take place via scheduled meetings, ad hoc conversations, internal announcements, and internal change control processes.

5. Estimated Project Cost

Category	Cost
Internal Cost (Salaries)	$0
Contractual Services	$352,378
Commodities	$0
Capital Outlay	$0
Sub-Total Project Costs	$352,378
Total KITO Rate Fee	$123
Total Project Costs	**$352,501**

KITO Rate Structure

Project Value Range		Quarterly Rate
$250,000	$10,000,000	0.00350
$10,000,001	Greater	0.00050
Infrastructure Projects		0.00035

Project Quarterly KITO Fee: $123

6. Project Subprojects (include name, start and end dates, and cost of each Subproject):

Subproject Name	Start Date	End Date	Internal Cost	External Cost	Total Cost
Planning	5/26/2022	1/20/2023	$0	$0	$0
Execution					
Build	1/16/2023	4/27/2023		$352,501	$352,501
Monitor	2/17/2023	4/4/2023		$0	$0
Control	4/17/2023	4/28/2023			$0
Enter Subproject 4 Name if Applicable					$0
Enter Subproject 5 Name if Applicable					$0
Execution Sub-Total	1/16/2023	4/28/2023	$0	$352,501	$352,501
Close-Out	4/26/2023	5/19/2023	$0	$0	$0
Grand Internal, External, and Total Costs			$0	$352,501	**$352,501**

7. Amount by Source of Financing:

State Fiscal Years	1. SGF	2. KUMC	3.	4.	5.	6.	7.	Total
SFY 2023	$352,378	$123						$352,501
SFY 2024								$0
SFY 2025								$0
SFY 2026								$0
SFY 2027								$0
SFY 2028								$0
Total Project Costs	$352,378	$123	$0	$0	$0	$0	$0	**$352,501**

Description of funds listed above

Revised 5/22

INFORMATION TECHNOLOGY PROJECT REQUEST EXPLANATION -- DA 519

1. Project Title	2. Estimated Dates		Projected Months from Execution to Close-Out
KUMC - Security Infrastructure - SIEM	Planning Start:	5/26/2022	5
	Execution Start:	1/16/2023	
	Close-Out End:	5/19/2023	

3. Agency	4. Project Director/Project Manager
Kansas University Medical Center	Jeremy Pennington / James Dillon

5. Qualitative and Quantitative Savings Explanation

The primary qualitative savings derived from this project are the result of enhancements to communication and collaboration. These qualitative savings will further be realized through the enhancements to KUMC business processes, improved student learning, facilitation of collaboration for research, and improved communications abilities by and between KUMC and collaborators.

Quantitative savings are driven primarily from cost avoidance of negative event realization. There will be additional quantitative savings from cost avoidance from a patchwork of alternative solutions to the SIEM, if the SIEM were not to be implemented/replaced. Other intangible benefits could add further to the quantitative savings identified.

6. Qualitative and Quantitative Savings Estimate

Description of Savings		SFY 2023	SFY 2024	SFY 2025	SFY 2026	SFY 2027	SFY 2028
Cost Avoidance (Soft Dollars)							
Unprevented Intrusion		$2,000,000	$3,250,000	$3,250,000	$4,000,000	$4,000,000	
Lack of trust by partners		$375,000	$500,000	$500,000	$500,000	$750,000	
Response to negative audit findings		$500,000	$750,000	$1,000,000	$1,000,000	$1,250,000	
Subtotal	$23,625,000	$2,875,000	$4,500,000	$4,750,000	$5,500,000	$6,000,000	$0
Cash Savings (Hard Dollars)							
Replacing End of Life System with more mature vendor		$0					
Subtotal	$0	$0	$0	$0	$0	$0	$0
Other (Include Intangible Benefits)							
Enhanced State and Federal Compliance		$125,000	$250,000	$250,000	$250,000	$250,000	
Improvement in detection and response		$325,000	$450,000	$450,000	$550,000	$550,000	
Subtotal	$3,450,000	$450,000	$700,000	$700,000	$800,000	$800,000	$0
Quantitative Savings	$27,075,000	$3,325,000	$5,200,000	$5,450,000	$6,300,000	$6,800,000	$0

7. Summary*		SFY 2023	SFY 2024	SFY 2025	SFY 2026	SFY 2027	SFY 2028
Project Costs	**Total** $352,501	$352,501	$0	$0	$0	$0	$0
Net Cost Benefit	**Total** $26,722,499	$2,972,499	$5,200,000	$5,450,000	$6,300,000	$6,800,000	$0
Cost Benefit per Month	$5,415,000						
Calendar Months to Break Even	0						

8. Ongoing Cost	SFY 2023	SFY 2024	SFY 2025	SFY 2026	SFY 2027	SFY 2028
Operational Cost for three ensuing SFYs		$0	$0	$0	$0	$0

* Project Costs = Total Cost of Project over all Fiscal Years from all Funding Sources
Net Cost Benefit = Total Qualitative & Quantitative Savings minus Total Project Costs
Cost Benefit per Month = Total Qualitative & Quantitative Savings divided by Length of Project in months
Calendar Months to Break Even = Total Project Costs divided by Cost Benefit per Month

Project Management Plan: Work Product Identification

Deliverable Name	*Due Date*	*Date Delivered*	*Point of Contact*
CITO High Level PP Approval 1.1.5 – (N/A – See Note)	N/A	N/A	J Dillon
Determine Vendor 1.3.6	7/15/2022	7/18/2022	J Beeson
Project Planning Complete 1.6	01/20/2023	1/20/2023	J Dillon
Testing Complete 2.1.2.5.5	04/27/2023		B Shoults
Communication Complete 2.1.2.7.4	04/04/2023		J Sells
Deployment Complete 2.2.1.9	04/04/2023		B Shoults
Execution/Monitor/Control Complete 2.3.3	04/24/2023		B Shoults
Customer acceptance and sign off 3.2	04/26/2023		J Dillon
Project Close Out Complete 3.7	05/19/2023		J Dillon
NOTE – Per Cover Letter – UKHS had started the project and determined a vendor prior to KUMC agreeing to partner in the project and use the same vendor for SIEM functionality.			

ID	Outline Number	Task Name	Duration	Work	Start	Finish	Predecessors	Resource Names	Milestone
0	**0**	**KUMC - Security Infrastructure - SIEM**	**255 days?**	**1,753.67 hrs**	**Thu 5/26/22**	**Fri 5/19/23**			**No**
1	**1**	**Planning**	**170 days**	**804 hrs**	**Thu 5/26/22**	**Fri 1/20/23**			**No**
2	**1.1**	**CITO Approvals**	**14 days**	**124 hrs**	**Thu 12/1/22**	**Tue 12/20/22**			**No**
3	1.1.1	N/A - KITO IT Planned Project Approval	1 day	8 hrs	Thu 12/1/22	Thu 12/1/22		Dillon	No
4	1.1.2	N/A - Prepare KITO High Level Project Materials	7.5 days	60 hrs	Thu 12/1/22	Mon 12/12/22		Dillon	No
5	1.1.3	KITO Approval of Web Accessibility Materials	5 days	8 hrs	Thu 12/8/22	Wed 12/14/22		KITO	No
6	1.1.4	KITO Approval of Electronic Record Retention Materials	8 days	8 hrs	Thu 12/8/22	Mon 12/19/22		KITO	No
7	1.1.5	N/A - CITO Approval of High Level Project Materials	5 days	40 hrs	Wed 12/14/22	Tue 12/20/22		CITO	No
8	**1.2**	**SIEM Vendor Acquisition**	**5 days**	**40 hrs**	**Thu 5/26/22**	**Wed 6/1/22**			**No**
9	1.2.1	Create RFP	3 days	24 hrs	Thu 5/26/22	Mon 5/30/22		J Beeson	No
10	1.2.2	Forward RFP to Purchasing	1 day	8 hrs	Tue 5/31/22	Tue 5/31/22	9	J Beeson	No
11	1.2.3	Post RFP	1 day	8 hrs	Wed 6/1/22	Wed 6/1/22	10	Purchasing	No
12	**1.3**	**Monitor Vendor Response**	**21 days**	**416 hrs**	**Mon 6/20/22**	**Mon 7/18/22**			**No**
13	1.3.1	Vendor Response - StellarCyber	10 days	80 hrs	Mon 6/20/22	Fri 7/1/22	11	Jim McGovern	No
14	1.3.2	Vendor Response - Cybraics	10 days	80 hrs	Mon 6/20/22	Fri 7/1/22	11	Carl Lucas	No
15	1.3.3	Vendor Response - Devo	10 days	80 hrs	Mon 6/20/22	Fri 7/1/22	11	Jerry Matt	No
16	1.3.4	Vendor Response - Elastic Security	10 days	80 hrs	Mon 6/20/22	Fri 7/1/22	11	Unknown	No
17	1.3.5	Vendor Response - Exabeam	10 days	80 hrs	Mon 6/20/22	Fri 7/1/22	11	Luke Voigt	No
18	1.3.6	**Determine Vendor**	2 days	16 hrs	Fri 7/15/22	Mon 7/18/22		J Beeson	Yes
19	**1.4**	**Detail Planning**	**38 days**	**148 hrs**	**Tue 11/1/22**	**Thu 12/22/22**			**No**
20	1.4.1	Prepare KITO Detail Level Project Materials	10 days	80 hrs	Tue 11/1/22	Mon 11/14/22		Dillon	No
21	1.4.2	CITO Approval of Detail Level Project Materials	11 days	40 hrs	Tue 12/6/22	Tue 12/20/22		C Robison	No
22	1.4.3	Prepare Project Team Kickoff Meeting	2.5 days	20 hrs	Tue 11/1/22	Thu 11/3/22		Dillon	No
23	1.4.4	Conduct Project Team Kickoff Meeting	1 day	8 hrs	Thu 12/22/22	Thu 12/22/22		Dillon	No
24	**1.5**	**Project Management**	**48 days**	**68 hrs**	**Mon 11/14/22**	**Fri 1/20/23**			**No**
25	1.5.1	Exabeam schedule weekly update calls	1 day	8 hrs	Mon 11/14/22	Mon 11/14/22		Berkley	No
26	1.5.2	Exabeam solution architecture overview	1 day	8 hrs	Mon 11/21/22	Mon 11/21/22		Berkley	No
27	1.5.3	Discuss implementation standards and process	1 day	8 hrs	Mon 11/28/22	Mon 11/28/22		Shoults	No
28	1.5.4	OIS Engineers schedule weekly update calls	1 day	8 hrs	Mon 11/14/22	Mon 11/14/22		Dillon	No
29	1.5.5	Communication	2 days	16 hrs	Tue 12/20/22	Wed 12/21/22		Dillon	No
30	1.5.6	Establish a Core Project Team	5 days	10 hrs	Mon 1/16/23	Fri 1/20/23		Dillon	No
31	1.5.7	Establish Risk Mitigation	5 days	10 hrs	Mon 1/16/23	Fri 1/20/23		Gaddie	No
32	1.6	**Project Planning Complete**	1 day	8 hrs	Fri 1/20/23	Fri 1/20/23		Dillon	Yes
33	**2**	**Execution**	**74 days?**	**916.67 hrs**	**Mon 1/16/23**	**Fri 4/28/23**			**No**
34	**2.1**	**Build Phase**	**73 days?**	**510.67 hrs**	**Mon 1/16/23**	**Thu 4/27/23**			**No**
35	**2.1.1**	**Detail Excution**	**35 days**	**178.67 hrs**	**Mon 1/16/23**	**Mon 3/6/23**			**No**

ID	Outline Number	Task Name	Duration	Work	Start	Finish	Predecessors	Resource Names	Milestone
36	**2.1.1.1**	**Documentation**	**31.5 days**	**66.67 hrs**	**Mon 1/16/23**	**Wed 3/1/23**	**18**		**No**
37	**2.1.1.1.1**	**Implementation Manifest**	**5 days**	**26.67 hrs**	**Wed 2/22/23**	**Wed 3/1/23**			**No**
38	2.1.1.1.1.1	Datasources - Tags and Application per datasource	5 days	13.33 hrs	Wed 2/22/23	Wed 3/1/23		Shoults	No
39	2.1.1.1.1.2	Logs - Expected per Application and Custom Parsers	5 days	13.33 hrs	Wed 2/22/23	Wed 3/1/23		Shoults	No
40	2.1.1.1.2	On-Prem Infrastructure	3 days	8 hrs	Thu 1/19/23	Fri 2/3/23		Shoults	No
41	2.1.1.1.3	Exabeam Cloud Configuration	3 days	24 hrs	Mon 1/16/23	Wed 1/18/23		Shoults	No
42	2.1.1.1.4	Collector Configuration	3 days	8 hrs	Thu 1/19/23	Fri 2/3/23		Shoults	No
43	**2.1.1.2**	**Reporting**	**11 days**	**56 hrs**	**Mon 2/6/23**	**Mon 2/20/23**			**No**
44	2.1.1.2.1	Replicate current reports	2 days	16 hrs	Fri 2/17/23	Mon 2/20/23		Shoults	No
45	2.1.1.2.2	Creation of new reports	5 days	40 hrs	Mon 2/6/23	Fri 2/10/23		Shoults	No
46	**2.1.1.3**	**Dashboards**	**17 days**	**56 hrs**	**Fri 2/10/23**	**Mon 3/6/23**			**No**
47	2.1.1.3.1	Replicate current dashboards	2 days	16 hrs	Fri 3/3/23	Mon 3/6/23		Shoults	No
48	2.1.1.3.2	Creation of new dashboards	5 days	40 hrs	Fri 2/10/23	Thu 2/16/23		Shoults	No
49	**2.1.2**	**Build**	**69 days?**	**332 hrs**	**Mon 1/23/23**	**Thu 4/27/23**			**No**
50	2.1.2.1	Analytics/Datalake Routing Split	3 days	24 hrs	Mon 1/23/23	Mon 4/10/23		Shoults	No
51	2.1.2.2	Logging Host verification	3 days	24 hrs	Wed 1/25/23	Tue 4/11/23		Shoults	No
52	2.1.2.3	Importation of Custom Parsers	3 days	24 hrs	Fri 1/27/23	Wed 4/12/23		Shoults	No
53	2.1.2.4	Context Table Generation	3 days	24 hrs	Tue 1/31/23	Thu 2/2/23		Shoults	No
54	**2.1.2.5**	**Testing**	**48 days?**	**164 hrs**	**Tue 2/21/23**	**Thu 4/27/23**			**No**
55	2.1.2.5.1	Test per Source Collectors	5 days	20 hrs	Thu 4/13/23	Wed 4/19/23		Shoults	No
56	2.1.2.5.2	Test and Compare Current and New Functionality	5 days	20 hrs	Thu 4/20/23	Wed 4/26/23	55	Shoults	No
57	2.1.2.5.3	DC Agent	5 days	20 hrs	Tue 2/21/23	Wed 3/8/23		Shoults	No
58	**2.1.2.5.4**	**Validate CASB Accessibility Requirements**	**2 days?**	**96 hrs**	**Mon 2/27/23**	**Tue 2/28/23**			**No**
59	**2.1.2.5.4.1**	**Validate Perceivability**	**1 day?**	**32 hrs**	**Mon 2/27/23**	**Mon 2/27/23**			**No**
60	2.1.2.5.4.1	Validate Text Alternatives	1 day	8 hrs	Mon 2/27/23	Mon 2/27/23		Berkley	No
61	**2.1.2.5.4.1**	**Validate Time-based Media**	**1 day?**	**8 hrs**	**Mon 2/27/23**	**Mon 2/27/23**			**No**
62	2.1.2.5.4.1	Audio/video/captions/other media alterna	1 day?	8 hrs	Mon 2/27/23	Mon 2/27/23		Berkley	No
63	2.1.2.5.4.1	Validate Adaptability	1 day	8 hrs	Mon 2/27/23	Mon 2/27/23		Berkley	No
64	**2.1.2.5.4.1**	**Validate Distinguishability**	**1 day**	**8 hrs**	**Mon 2/27/23**	**Mon 2/27/23**			**No**
65	2.1.2.5.4.1	Color/Audio/ text size/contrast	1 day	8 hrs	Mon 2/27/23	Mon 2/27/23		Berkley	No
66	**2.1.2.5.4.2**	**Validate Operability**	**1 day**	**32 hrs**	**Tue 2/28/23**	**Tue 2/28/23**			**No**
67	2.1.2.5.4.2	Validate Keyboard Accessible	1 day	8 hrs	Tue 2/28/23	Tue 2/28/23	65	Berkley	No
68	**2.1.2.5.4.2**	**Validate Enough Time**	**1 day**	**8 hrs**	**Tue 2/28/23**	**Tue 2/28/23**			**No**
69	2.1.2.5.4.2	Timing Adjustable/Pause,stop,hide/No tim	1 day	8 hrs	Tue 2/28/23	Tue 2/28/23	65	Berkley	No
70	2.1.2.5.4.2	Validate CASB has been designed as to not ca	1 day	8 hrs	Tue 2/28/23	Tue 2/28/23	65	Berkley	No
71	**2.1.2.5.4.2**	**Validate Navigatibility**	**1 day**	**8 hrs**	**Tue 2/28/23**	**Tue 2/28/23**			**No**
72	2.1.2.5.4.2	Bypass blocks/Page titled/Focus Order/Lin	1 day	8 hrs	Tue 2/28/23	Tue 2/28/23	65	Berkley	No
73	**2.1.2.5.4.3**	**Validate Understandability**	**1 day**	**24 hrs**	**Tue 2/28/23**	**Tue 2/28/23**			**No**
74	**2.1.2.5.4.3**	**Validate Readability**	**1 day**	**8 hrs**	**Tue 2/28/23**	**Tue 2/28/23**			**No**

ID	Outline Number	Task Name	Duration	Work	Start	Finish	Predecessors	Resource Names	Milestone
75	2.1.2.5.4.3	Language of page and parts/ unusual wor	1 day	8 hrs	Tue 2/28/23	Tue 2/28/23	65	Berkley	No
76	**2.1.2.5.4.3**	**Validate Predictability**	**1 day**	**8 hrs**	**Tue 2/28/23**	**Tue 2/28/23**			**No**
77	2.1.2.5.4.3	Focus/input/consistent navigation and ide	1 day	8 hrs	Tue 2/28/23	Tue 2/28/23	65	Berkley	No
78	2.1.2.5.4.3	Validate Input Assistance: Help users avoid a	1 day	8 hrs	Tue 2/28/23	Tue 2/28/23	65	Berkley	No
79	**2.1.2.5.4.4**	**Validate CASB content is Robust - Can be interpreted reliably**	**1 day**	**8 hrs**	**Tue 2/28/23**	**Tue 2/28/23**			**No**
80	**2.1.2.5.4.4**	**Validate Compatibility**	**1 day**	**8 hrs**	**Tue 2/28/23**	**Tue 2/28/23**			**No**
81	2.1.2.5.4.4	Parsing/Name,role,value	1 day	8 hrs	Tue 2/28/23	Tue 2/28/23	65	Berkley	No
82	2.1.2.5.5	Testing Complete	1 day	8 hrs	Thu 4/27/23	Thu 4/27/23	55,56	Shoults	Yes
83	**2.1.2.6**	**Training**	**9 days**	**24 hrs**	**Mon 3/20/23**	**Thu 3/30/23**			**No**
84	2.1.2.6.1	Office of Information Security	3 days	8 hrs	Mon 3/20/23	Wed 3/22/23		Sells	No
85	2.1.2.6.2	Server and Storage	3 days	8 hrs	Thu 3/23/23	Mon 3/27/23		Sells	No
86	2.1.2.6.3	Application Admin / System Admin	3 days	8 hrs	Tue 3/28/23	Thu 3/30/23		Sells	No
87	**2.1.2.7**	**Communication**	**2 days**	**48 hrs**	**Mon 4/3/23**	**Tue 4/4/23**			**No**
88	2.1.2.7.1	SIEM Updates	2 days	16 hrs	Mon 4/3/23	Tue 4/4/23		Sells	No
89	2.1.2.7.2	HelpDesk	2 days	16 hrs	Mon 4/3/23	Tue 4/4/23		Sells	No
90	2.1.2.7.3	Reporting with Server Admins	2 days	16 hrs	Mon 4/3/23	Tue 4/4/23		Sells	No
91	2.1.2.7.4	Communications Complete	1 day	0 hrs	Tue 4/4/23	Tue 4/4/23			Yes
92	**2.2**	**Monitor Phase**	**33 days**	**318 hrs**	**Fri 2/17/23**	**Tue 4/4/23**			**No**
93	**2.2.1**	**On-Prem Infrastructure Deployment**	**33 days**	**318 hrs**	**Fri 2/17/23**	**Tue 4/4/23**			**No**
94	**2.2.1.1**	**Server Build**	**5 days**	**48 hrs**	**Thu 3/9/23**	**Wed 3/15/23**			**No**
95	2.2.1.1.1	VM's Built	2 days	16 hrs	Thu 3/9/23	Fri 3/10/23		Shoults	No
96	2.2.1.1.2	OS Certification	2 days	16 hrs	Mon 3/13/23	Tue 3/14/23		Shoults	No
97	2.2.1.1.3	App Certification	2 days	16 hrs	Tue 3/14/23	Wed 3/15/23		Campbell	No
98	2.2.1.2	Log Type Tagging	2 days	16 hrs	Wed 3/15/23	Thu 3/16/23		Shoults	No
99	**2.2.1.3**	**Collectors installed**	**1.5 days**	**6 hrs**	**Tue 2/21/23**	**Wed 2/22/23**			**No**
100	2.2.1.3.1	Install New Gen Collectors	1 day	4 hrs	Tue 2/21/23	Tue 2/21/23		Shoults	No
101	2.2.1.3.2	Connect collectors to Exabeaan cloud environmer	0.5 days	2 hrs	Wed 2/22/23	Wed 2/22/23		Shoults	No
102	**2.2.1.4**	**Load Balance Setup**	**4 days**	**24 hrs**	**Mon 3/20/23**	**Thu 3/23/23**			**No**
103	2.2.1.4.1	Determine Forwarding Method	1 day	8 hrs	Mon 3/20/23	Mon 3/20/23		Shoults	No
104	2.2.1.4.2	Host maintenance procedures	1 day	8 hrs	Tue 3/21/23	Tue 3/21/23		Shoults	No
105	2.2.1.4.3	Host restart procedures	1 day	8 hrs	Thu 3/23/23	Thu 3/23/23		Shoults	No
106	**2.2.1.5**	**Collector Configuration**	**5 days**	**16 hrs**	**Wed 3/22/23**	**Tue 3/28/23**			**No**
107	2.2.1.5.1	DC Agent Test	1 day	4 hrs	Wed 3/22/23	Wed 3/22/23		Berkley	No
108	2.2.1.5.2	Host down notification configuration	1 day	8 hrs	Mon 3/27/23	Mon 3/27/23		Berkley	No
109	2.2.1.5.3	Certificates Generated and Deployed	1 day	4 hrs	Tue 3/28/23	Tue 3/28/23		Berkley	No
110	**2.2.1.6**	**KUMC/UKHS Implementation Details**	**8 days**	**32 hrs**	**Wed 3/22/23**	**Fri 3/31/23**			**No**
111	2.2.1.6.1	Tenant incoming lod metrics impact	1 day	8 hrs	Wed 3/29/23	Wed 3/29/23		Shoults	No
112	2.2.1.6.2	Datasource restrictions table built and implemented for KUMC data only	1 day	8 hrs	Thu 3/30/23	Thu 3/30/23		Shoults	No
113	2.2.1.6.3	KUMC personnel Integration	1 day	8 hrs	Fri 3/31/23	Fri 3/31/23		Shoults	No

ID	Outline Number	Task Name	Duration	Work	Start	Finish	Predecessors	Resource Names	Milestone
114	2.2.1.6.4	Fusion Center Integration Verification	1 day	8 hrs	Wed 3/22/23	Wed 3/22/23		Shoults	No
115	2.2.1.7	Soft Restart Protocol for Hosts	1 day	8 hrs	Mon 4/3/23	Mon 4/3/23		Shoults	No
116	2.2.1.8	Per Source Collectors	1 day	8 hrs	Tue 4/4/23	Tue 4/4/23		Shoults	No
117	2.2.1.9	Deployment Complete	1 day	0 hrs	Tue 4/4/23	Tue 4/4/23			Yes
118	2.2.1.10	Monitor and Recover SIEM Service Outage Rapidly V	5 days	40 hrs	Fri 2/17/23	Thu 2/23/23		Proj Team	No
119	2.2.1.11	Monitor and Recover SIEM Service Outage Rapidly V	5 days	40 hrs	Fri 2/24/23	Thu 3/2/23		Proj Team	No
120	2.2.1.12	Monitor and Recover SIEM Service Outage Rapidly V	5 days	40 hrs	Fri 3/3/23	Thu 3/9/23		Proj Team	No
121	2.2.1.13	Monitor and Recover SIEM Service Outage Rapidly V	5 days	40 hrs	Fri 3/10/23	Thu 3/16/23		Proj Team	No
122	**2.3**	**Control Phase**	**10 days**	**88 hrs**	**Mon 4/17/23**	**Fri 4/28/23**			**No**
123	2.3.1	Validate Deliverables	5 days	40 hrs	Mon 4/24/23	Fri 4/28/23		Proj Team	No
124	2.3.2	Validate Issue Repairs	5 days	40 hrs	Mon 4/17/23	Fri 4/21/23		Proj Team	No
125	2.3.3	Execution / Monitor / Control Complete	1 day	8 hrs	Mon 4/24/23	Mon 4/24/23	124	Dillon	Yes
126	**3**	**Close-Out**	**18 days**	**33 hrs**	**Wed 4/26/23**	**Fri 5/19/23**			**No**
127	3.1	Conduct Lessons Learned Sessions	8 days	8 hrs	Wed 4/26/23	Fri 5/5/23	125	Dillon	No
128	3.2	Customer Acceptance Signoff	1 day	8 hrs	Wed 4/26/23	Wed 4/26/23		Dillon	Yes
129	3.3	Archive Project Records	8 days	4 hrs	Fri 5/5/23	Tue 5/16/23	127	Dillon	No
130	3.4	Draft PIER Report	8 days	8 hrs	Fri 5/5/23	Tue 5/16/23	129	Dillon	No
131	3.5	Submit PIER to CITO	8 days	1 hr	Fri 5/5/23	Tue 5/16/23		Dillon	No
132	3.6	Celebrate Plan Completion	10 days	3 hrs	Fri 5/5/23	Thu 5/18/23		Dillon	No
133	3.7	Close Out Complete	1 day	1 hr	Fri 5/19/23	Fri 5/19/23		Dillon	Yes

State Archives Division
6425 SW 6th Avenue
Topeka KS 66615-1099

Kansas Historical Society

785-272-8681, ext. 272
megan.burton@ks.gov
kshs.org

Patrick Zollner, Acting Executive Director

Laura Kelly, Governor

December 14, 2022

Jeremy Pennington, Chief Information Security Officer
The University of Kansas Medical Center
4330 Shawnee Mission Pkwy.
Fairway, KS 66205

Dear Mr. Pennington,

As part of the approval process for information technology projects over $250,000, the State Archivist is required to evaluate the impact of information technology projects on government records with long-term (10+ year) retention requirements. If the project impacts long-term records, the State Archivist must ensure that appropriate provisions have been made for these records in the high-level and detailed project plans, in the system design, and for their ingestion, if prudent and feasible, into the Kansas Enterprise Electronic Preservation (KEEP) system. An Electronic Records Retention Statement and approval letter from the State Archivist must accompany high-level and detailed project plans submitted to the Executive Branch Chief Information Technology Officer.

In compliance with this process, James Dillon, Project Manager, recently sent to me for review an Electronic Records Retention Statement for the KUMC Security Information and Event Management (SIEM) Information Security Infrastructure detail-level plan. It is clear that this is an infrastructure only plan and does not impact records.

The Electronic Records Retention Statement for the detail-level plan is approved. A copy of this approval letter should be included when submitting the project plan to the Executive Branch CITO for approval.

Sincerely,

Ethan Anderson
Government Records Archivist

Cc: Cole Robison, Director of IT Accessibility, OITS
James Dillon, Project Manager, KUMC

Executive Branch Information Technology
Office of Information Technology Services
2800 SW Topeka Blvd., Building 100
Topeka, KS 66611

Kansas
Office of Information Technology Services

Phone: (785) 296-3463
Fax: (785) 296-1168
oits.info@ks.gov

Jeff Maxon, Interim Chief Information Technology Officer

Laura Kelly, Governor

February 24, 2023

Jeremy Pennington, Chief Information Security Officer (CISO)
The University of Kansas Medical Center
4330 Shawnee Mission Pkwy.
Fairway, Kansas 66205

Dear Mr. Pennington:

As part of the approval process for information technology projects over $250,000, a statement indicating compliance with State Information Technology Executive Council (ITEC) Policy 1210 *Information and Communication Technology Accessibility Standards* must be filed with the Branch Chief Information Technology Officer and approved by the Director of Information Technology (IT) Accessibility. I recently received from James Dillon an Accessibility Statement for the KUMC - Security Infrastructure – SIEM project for review in compliance with this process.

This Accessibility Statement is accompanied by an exception to ITEC Policy 1210, which was granted by State ADA Coordinator Anthony Fadale for this project, and which I have also received. The Accessibility Conformance Report (ACR) for the product involved shows incomplete compliance, necessitating this exception.

Consistent with this exception, and subject to the conditions outlined therein, the Accessibility Statement requirement for the KUMC - Security Infrastructure – SIEM detailed project plan is satisfied. All components of the project should be made to achieve as much compliance with ITEC Policy 1210 as possible within the limitations of the products, and appropriate alternative accommodation should be provided if needed.

A copy of this letter should be included with the submittal of the KUMC - Security Infrastructure – SIEM detailed project plan to the Branch CITO for approval.

Sincerely,

DocuSigned by:
Cole D. Robison
B7372BF57AD54B7...

Cole D. Robison
Director of IT Accessibility

cc: James Dillon, The University of Kansas Medical Center
Anthony Fadale, State Americans with Disabilities Act Coordinator
Chris Harper, The University of Kansas Medical Center
Sara Spinks, Director, Kansas Information Technology Office

November 21, 2022

RE: SIEM Project compliance statements for the University of Kansas Medical Center (KUMC)

This proposed project is designed to help KUMC implement the most appropriate hardware and software infrastructure for our requirements. This is an IT infrastructure project that entails implementing a security information and event management (SIEM) information security infrastructure.

The motivation for this project is the need for KUMC to upgrade and replace the current SIEM. The SIEM offers real-time monitoring and analysis of events as well as tracking and logging of security data for compliance or auditing purposes. SIEM will help enable KUMC support for security and compliance management requirements. SIEM, broadly speaking, is a security solution that will continue to help KUMC recognize potential security threats and vulnerabilities before they have a chance to disrupt business operations. It surfaces user behavior anomalies and uses artificial intelligence to automate many of the manual processes associated with threat detection and incident response. It will continue to provide KUMC with capability to prevent, monitor, and mitigate high-risk events for KUMC. The ability for KUMC to continue their work in improving lives and communities in Kansas and beyond through innovation in education, research, and health care is the business objective and the primary driver for this project.

Architectural Statement

KUMC follows ITEC Policies 4010 and 9500.

Architectural information for this proposed SIEM project follows the Kansas Information Technology Architecture version 12.0. This project entails the upgrade and replacement of the current SIEM which will capture all infrastructure logs. In house development and vendor supplied technologies will be implemented in accordance with State Architecture standards.

Ownership of Software Code and Related Intellectual Property Statement

KUMC follows ITEC Policy 1500.

This proposed project is an infrastructure project. There will not be any software code generated during the project. Accordingly, the project does not present any compliance issues with ITEC Policy 1500.

Privacy Compliance Statement

KUMC's privacy and related compliance requirements will remain in force for this project. Users and consumers of the project capabilities are required to comply with KUMC's policies and procedures pertaining to the high-risk HIPAA data environment.

Security Compliance Statement

KUMC follows ITEC Policies 7230 and 7230a.

This project is designed to help KUMC implement the most appropriate monitoring and analysis infrastructure for our requirements. This is an IT infrastructure project that entails implementing security infrastructure. The technologies and architecture of the proposed solution are mature. The proposed project follows the State of Kansas information security policies (i.e., ITEC 7230 and ITEC 7230a) and internal KUMC policies.

Accessibility Statement

This proposed SIEM project is an IT infrastructure project that entails replacing and implementing a SIEM information security infrastructure. This project will follow ITEC policies governing accessibility. A Voluntary Product Accessibility Template has been requested of the vendor and will be provided in a separate document.

Vendor and product selection processes will include an evaluation of accessibility compliance. In the event a fully compliant option was not selected, or does not meet the KUMC project business requirements, KUMC will seek an undue burden exception to cover the compliance gaps, as ITEC Policy 1210 (as found at https://ebit.ks.gov/itec/resources/policies/policy-1210) is supported with exceptions.

Electronic Record Retention Statement

This proposed SIEM project is an IT infrastructure project that entails implementing a SIEM information security infrastructure. Any record retention requirements within KUMC today will not be affected by this project and will remain in their current state. This project will not directly impact recordkeeping systems in place at KUMC.

1. For each business function supported by the new system, what paper records are being replaced and which will continue to exist in both paper and electronic form?

This project will not affect any electronic records. It is an infrastructure project involving the installation of information security infrastructure.

2. What new business functions will be implemented?

No new business functions will be implemented.

3. What are the reasons for performing the business functions?

N/A

4. What legal, regulatory, or operational requirements, including State Records Board approved retention schedules, exist for keeping records related to each business function?

N/A

5. Will any of the data necessary to document the business functions either be maintained in another system within the agency or in a system outside the agency? If so, please specify.

N/A

6. What are the legal, regulatory, or operational requirements to providing public access to the records?

N/A

7. What are the legal, regulatory, or operational requirements for controlling access to the records in order to ensure confidentially?

N/A

8. Identify all records with retention periods of ten or more years that will be affected by the project or indicate that the project has no such records involved.

N/A

9. Estimate of the three-year total cost of addressing records identified in No. 8 above and included on the DA519, Item #8.

N/A

Risk Identification Summary
(Top Five Risks)

A description of project risks, the probability of the risk occurring, the impact of the risk on the project, and the suggested mitigation activities.

Last Risk Assessment Date: 11/18/2022 Prepared by: James Dillon

Category	*Prob*	*Imp*	*Risk*	*Mitigation Approaches*
	Low	**High**	**Loss of critical resources**	**Either use contracted services or delay the project**
	Low	**High**	**Lack of vendor availability**	**Escalation to vendor management or delay of project timeline**
	Low	**High**	**Lack of Communication around scheduling**	**Closer Project Management involvement**
	Low	**Med**	**Inability to meet project milestones**	**Closer Project Management involvement and escalation with vendor**
	Low	**High**	**Accidental high-risk data exposure**	**Limit high risk data until after deployment, don't test live data. Complete use case testing.**

Legend
Prob = Probability of Occurrence
Imp = Impact

RISK ASSESSMENT MODEL
Detailed Plan - Summary Report
Ver. 1.0

Agency Name: Kansas University Medical Center

Project Name: KUMC - Security Infrastructure - SIEM

1. Introduction

The Risk Assessment Model measures risk in distinct areas. Below are the average scores based on the results from the questionnaire. Each area indicates the measured risk on a scale from 1 to 9, with 9 being the highest risk. Scores lower than 2.0 are considered "Low Risk", scores higher than 2.0 are "Medium Risk" and scores higher than 3.0 are considered "High Risk".

2. Summary

Score	Risk Level	Risk Area
1.4	LOW	Strategic Risk
1.3	LOW	Financial Risk
2.1	MEDIUM	Project Management Risk
1.4	LOW	Technology Risk
2.0	MEDIUM	Change Management / Operational Risk

Note: If you get "#VALUE!" as a result in any of the "Score" or "Risk Level" fields, you have unanswered questions. Go back and check your answers.

3. Signature

I have reviewed the results of the Risk Assessment Model. The results are indicators only and do not represent all the risks of the project. ITEC will use the results as the basis of discussion, and will not rely solely on the output.

James Dillon - Project Manager, KUMC Office of Information Security

Project Director

RISK ASSESSMENT - Summary Report

Detailed Plan - List of Comments

(Expand Row Height to Show all Text)

1	
2	
3	
4	
5	
6	
7	
8	
9	
10	
11	
12	
13	
14	
15	
16	
17	
18	Selected 3 due the new environment as a result of COVID-19
19	
20	
21	
22	
23	
24	
25	
26	
27	
28	
29	
30	
31	
32	
33	
34	
35	
36	
37	
38	