Name of Vendor

Cloud Service Provider Questionnaire

1. Does the Cloud Service Provider (CSP) have a secure environment, federally authorized to at least the standards of confidentiality and integrity from the Moderate FIPS-199 level to store records containing Personal Identifiable Information (PII)?

2. Does the Cloud provider have the ability to alter Terms of Service or contracts without the express written consent of the customer agency?

3. Will the ownership of data remain under the sole ownership of the State of Kansas at all times?

4. Will backup information be returned to the State of Kansas in the event the contract is ended or the Cloud provider files for bankruptcy?

5. Is there a documented process to address the removal and control of agency information upon the termination of the contract between the agency and the cloud provider?

6. Can the cloud provider utilize any data stored on their systems for any purpose outside agency use?

7. Does the contract contain language to restrict the sharing of privacy data with any entity not explicitly authorized in the contract?

8. Does the contract contain language to restrict the storage, transfer, or processing of privacy data to only facilities that fall under the legal jurisdiction of the United States?

9. What controls are in place to prevent the misuse of data by those having access?

10. Does the cloud provider allow for access to data as permitted under current federal and Kansas law to both authorized federal agencies and individuals wishing to verify their own PII?

11. While the data is with the cloud provider, what are the requirements for determining if the data is sufficiently accurate, relevant, timely, and complete to ensure fairness in making determinations?

12. Describe what privacy training is provided and who is responsible for protecting the privacy rights of the users of the cloud?

13. How does the cloud provider facilitate response to Kansas Open Records Act (KORA) / Federal Open Information Act (FOIA) / subpoena requests?

14. Is there a complete and documented process to report and handle breaches?

15. Describe the process that the CSP will use to report, within 1-hour, any potential privacy or security breaches to the agency regardless of whether the breach was intentional or inadvertent.

16. Describe the specific redress actions that the agency can take against the cloud provider in the event of a breach.

Security Questionnaire

Instructions for Completing the Web-Enabled Application Security Questionnaire
Vendor will complete this questionnaire by responding to all questions to the best of their ability.

Web-Enabled Application Security Questionnaire for: *Vendor Name* **Date:** / /		
Physical Security- involves the security of the physical devices, which includes the ability to control access to such hardware.		
#	**Question**	**Response**
1	What are the hardware components and where are they physically located?	
2	Who has access to the physical components?	
3	Are the environmental controls adequate (i.e., smoke and water detection, fire prevention)?	
4	What UPS is being used and what characteristics does it have?	
User Security- addresses the ability to ensure that the user accessing data and systems is in fact who they say they are and that they have access only to those resources to which they are authorized. Functions that are involved in this issue include identification, authentication, and authorization of the individual, as well as non-repudiation and audit.		
#	**Question**	**Response**
5	How are users identified to the systems?	
6	What unique form of identification do they have (UserID) ?	
7	Who administers the UserIDs?	
8	How are inactive users removed, by whom, and how timely?	
9	How are users authenticated to the system (passwords, smart cards, biometrics)?	
10	If passwords are used, what are the specific password rules (minimum length, character makeup, aging, etc)?	

Web-Enabled Application Security Questionnaire for: *Vendor Name* **Date:** / /		
11	How is assurance provided that the information received has not been altered?	
12	How is assurance provided that the reputed sender is indeed the one who sent it?	
13	What levels of system access are there?	
14	Who determines and maintains?	
15	What audit trails are maintained to enable reconstruction and/or review of operations performed on systems?	
16	How are they protected so users can not change them?	
17	How often are they reviewed and by whom?	
Application Security- concerns the built-in security features of the application itself.		
#	**Question**	**Response**
18	What security features are built into the application?	
19	How specifically do the security features work?	
20	If the application communicates to other systems, how does that happen? (i.e.. web server to database server).	
21	Has **auto complete = off** been set for all input fields on applications using IE 5.0 or above.?	
22	What information is logged for each transaction? (The minimum is userID, IP Address, and time and date stamp)	
23	Where is the logging information stored?	

Web-Enabled Application Security Questionnaire for: *Vendor Name* **Date:** / /		
24	Does the application use session tokens that are custom created or default from a Vendor, i.e.. Microsoft? (All session tokens shall be user unique, non-predictable, and resistant to reverse engineering.)	
25	Does the application store any cookies on client machines? If so, what are they?	
26	Are cookies checked for validity when returned back to the server?	
27	Are sessions and/or cookies destroyed when the user logs out of the application?	
28	Does the application require re-authentication for critical user actions such as money transfer?	
29	What security controls are built around files where userIDs, passwords, Pins, etc are stored?	
30	Are all authentication events (logging in, logging –out, failed logins, etc.) logged?	
31	Are all administrative events (account management actions, enabling or disabling logging, etc.) logged?	
32	Are logs written so only new records can be added, and existing records not overwritten or deleted?	
33	What client-side data validation is done?	
34	What data validation is done on the server side? (this shall be done even if it is redundant to cursory validation performed on the client side).	

Web-Enabled Application Security Questionnaire for: *Vendor Name* **Date:** / /		
35	How is editing done to prohibit generic meta-characters from being present in input data?	
36	Are all database queries constructed with parameterized stored procedures to prevent SQL injection?	
37	Can any variables be used in script? If yes, how are they protected to prevent direct OS Commands attacks?	
38	What scripting language is being used? Has it been checked for vulnerabilities and have they been addressed?	
39	Does the application do security checking after UTF-8 decoding is completed?	
40	Have all comments been removed for any code passed to the browser?	
41	Can users see any debugging information on the client?	
42	Have all sample, test and unused files been removed from the production system?	
43	Are pages with personal data cached?	
44	Are forms submissions done using a POST request rather than a GET?	
45	Does IUSR and/or network services need write permissions to any folders? If so, which ones and why?	
46	Does IUSR and/or Network Service need read and/or write access to the registry beyond the defaults?	

Web-Enabled Application Security Questionnaire for: *Vendor Name* **Date:** / /		
47	Does your application require any shared folders?	
48	Are all your connection string information(passwords & user names) stored in the registry and not in the application?	
49	Does your application need parental paths on in the IIS server?	
50	Does your application use stored procedures for database interaction?	
51	Do you follow ADA guidelines in your presentation layers of your application?	
52	Does your application require any 3rd party software that is not a standard part of our Microsoft operating system?	
53	Does your web application adhere to a three layer architecture (Presentation, Business and Data)?	
System Security-involves the analysis of the overall operating systems and software used to support the applications software.		
#	**Question**	**Response**
54	What research has been done for known security vulnerabilities?	
55	Who installs Vendor-supplied security upgrades and patches? Are we up-to-date?	
56	Have unnecessary services been removed or disabled?	
57	Has debugging mode on any web server been turned off for production?	
58	Are default accounts disabled and passwords changed from defaults?	

Web-Enabled Application Security Questionnaire for: *Vendor Name* **Date:** / /		
59	Does the data base user have limited abilities in being only able to run stored procedures or select?	
Data Security-encompasses both physically protecting the application data from unauthorized access as well as loss of data through mechanical/electrical failure or viruses		
#	**Question**	**Response**
60	Is Authentication used at all times when accessing or making changes to data to ensure confidentiality?	
61	Is at least 128-bit encryption used for any data transmitted over public networks?	
62	Are all FTP transmissions of data over insecure channels encrypted using PGP software?	
63	Is auditing activated and all access to data logged?	
64	What are the backup and archive procedures that will be used?	
65	What are the offsite storage requirements of backups and archives?	
66	Are backups encrypted if highly sensitive data is involved?	
67	What virus control software and detection procedures will be used to protect the data?	
68	How is privacy maintained to ensure that customer's personal data collected from electronic transmissions is protected from unauthorized transmissions?	
Network Security-.includes the physical/electrical links between the Desktop Client and the Host computer		
#	**Question**	**Response**

Web-Enabled Application Security Questionnaire for: *Vendor Name* **Date:** / /		
69	What documents show the network environment with a diagram that shows all links and component parts?	
70	How is the LAN isolated from any network-connected device that does not have a valid business relationship with resources on the LAN?	
71	Are firewalls used between the LAN and the Internet to prevent untrusted networks from accessing the LAN?	
72	If public access to a server in the internal LAN is required, has the server been put on a separate LAN segment behind the firewall device typically referred to as the DMZ?	
73	Have intrusion detection systems been installed?	
74	How are they monitored for unauthorized access?	
Security Administration- involves the administration of the overall security plan		
#	**Question**	**Response**
75	Who are the security administrators for the application?	
76	What functions do they provide?	
77	How are users provided with userIDs and passwords?	
78	Are passwords restricted from being distributed by telephone or unsecured electronic mail?	
79	How are unusual incidents handled?	

Web-Enabled Application Security Questionnaire for: *Vendor Name* **Date:** / /		
80	Have all employees or users of the application been instructed to exercise caution to prevent the release of sensitive details to unauthorized sources?	
Database Security: involves the connections to the database		
#	**Question**	**Response**
81	Do you pass SQL query information or hierarchy paths via the request objects?	
82	Does your application use server side validation for sensitive, financial, or authorization information input before disseminating, writing, updating or allowing access to the application or database?	

Architecture Document

Vendor Name

Date