623 SW 10th Avenue
Topeka, KS 66612
(800) 232-2259
www.kammco.com

Cyber Breach Response Application

NOTICE: This policy's liability insuring agreements provide coverage on a claims made and reported basis and apply only to claims first made against the insured during the policy period or the optional extension period (if applicable) and reported to the underwriters in accordance with the terms this policy. Amounts incurred as claims expenses under this policy will reduce and may exhaust the limit of liability and are subject to retentions.

Read this policy carefully, and answer all questions.

Please return this application, along with any necessary attachments,
by email to underwriting@kammco.com or by fax to 785.232.4704.

If you work with a KAMMCO agent, please submit this application directly to your agent.

Requested Effective Date (MM/DD/YYYY): _____

GENERAL INFORMATION		
Full Name:		
Mailing Address:		State of Incorporation:
City:	State:	Zip:
Number of Employees:	Date Established:	
Website URLs:		
Authorized Officer[1] Name:	Phone:	
	Email:	
Breach Response Contact[2] Name:	Phone:	
	Email:	
Business Description:		
Does the Applicant provide data processing, storage, or hosting services to third parties?	☐ Yes ☐ No	

[1]This is the officer of the Applicant that is authorized make statements to the Underwriters on the Applicant's behalf and to receive notices from the Insurer or its authorized representative(s).

[2]This is the employee of the Applicant that is designated to work with the insurer in response to a data breach event.

REVENUE INFORMATION

Net Patient Services Revenue plus Other Operating Revenue

	Most Recent Twelve (12) months: (Ending): _____ / _____	Previous Year	Next Year (estimate)
US Revenue:	**USD**	**USD**	**USD**
Non-US Revenue:	**USD**	**USD**	**USD**
Total:	**USD**	**USD**	**USD**

Please attach a copy of your most recently audited annual financial statement.

What percentage of the Applicant's revenues are business to business?	% _____
What percentage of the Applicant's revenues are direct to consumer?	% _____
Are significant changes in the nature or size of the Applicant's business anticipated over the next twelve (12) months? Or have there been any such changes within the past twelve (12) months? If yes, please explain: _____	☐ Yes ☐ No
Has the Applicant within the past twelve (12) months completed or agreed to, or does it contemplate entering into within the next twelve (12) months, a merger, acquisition, consolidation, whether or not such transactions were or will be completed? If yes, please explain: _____	☐ Yes ☐ No

PRIVACY AND COMPUTER & NETWORK SECURITY

Does the Applicant have and require employees to follow written computer and information systems policies and procedures?	☐ Yes ☐ No
Does the Applicant use the following controls:	
Commercially available Firewall protection?	☐ Yes ☐ No
Commercially available Anti-Virus protection?	☐ Yes ☐ No
If no, please describe the alternative controls implemented to prevent unauthorized access or intrusion to Computer Systems: _____	
Does the Applicant terminate all computer access and user accounts as part of the regular exit process when an employee leaves the company or when a third party contractor no longer provides the contracted services?	☐ Yes ☐ No
Does the Applicant accept credit cards for goods sold or services rendered?	☐ Yes ☐ No
If yes, please state the Applicant's approximate percentage of revenues from credit card transactions within the past twelve (12) months:	% _____
Is the Applicant compliant with applicable data security standards issued by financial institutions with which the Applicant transacts business (e.g., PCI standards)?	☐ Yes ☐ No

Does the Applicant have and enforce policies concerning the encryption of internal and external communication?	☐ Yes ☐ No
Are users able to store data to the hard drive of portable computers or portable media devices such as USB drives?	☐ Yes ☐ No
Does the Applicant encrypt data stored on laptop computers and portable media?	☐ Yes ☐ No
Please describe any additional controls the Applicant has implemented to protect data stored on portable devices: _____	

What format does the Applicant utilize for backing up and storage of computer system data?

☐ Tape or other media ☐ Online backup service ☐ Other: _____

Are tapes or other portable media containing backup materials encrypted?	☐ Yes ☐ No
Are tapes or other portable media stored offsite using secured transportation and secured storage facilities?	☐ Yes ☐ No
If stored offsite, are transportation logs maintained?	☐ Yes ☐ No
If stored onsite, please describe physical security controls: _____	

MEDIA CONTROLS

Please describe the media activities of the Applicant or by others on behalf of the Applicant.

☐ Television ☐ Radio ☐ Print ☐ Applicant's Website(s) ☐ Internet Advertising ☐ Social Media

☐ Marketing Materials ☐ Audio or Video Streaming ☐ Other: _____

Does the Applicant have a formal review process in place to screen any published or broadcast material (including digital content), for intellectual property and privacy compliance prior to any publication, broadcast, distribution or use?	☐ Yes ☐ No ☐ N/A
Are such reviews conducted by, or under the supervision, of a qualified attorney?	☐ Yes ☐ No ☐ N/A
Does the Applicant allow user generated content to be displayed on its website(s)?	☐ Yes ☐ No ☐ N/A

RANSOMWARE

1. How often is phishing training conducted to all staff: _____

   When was the last such training completed: _____

2. Do you strictly enforce Sender Policy Framework (SPF) on incoming e-mails?	☐ Yes ☐ No ☐ N/A
3. Do you pre-screen emails for potentially malicious attachments and links?	☐ Yes ☐ No ☐ N/A
4. Do you provide a quarantine service to your users?	☐ Yes ☐ No ☐ N/A
5. Do you have the capability to automatically detonate and evaluate attachments in a sandbox to determine if malicious prior to delivery to the end-user?	☐ Yes ☐ No ☐ N/A
6. Can users run MS Office Macro enabled documents on their system by default?	☐ Yes ☐ No ☐ N/A

7. Do you use Office 365 in your organization? *If yes, do you use the o365 Advanced Threat Protection add-on?*	☐ Yes ☐ No ☐ N/A ☐ Yes ☐ No ☐ N/A
8. Do you use an endpoint protection (EPP) product across your enterprise?	☐ Yes ☐ No ☐ N/A
9. Do you use an endpoint detection and response (EDR) product across your enterprise?	☐ Yes ☐ No ☐ N/A
10. Do you use an endpoint application isolation and containment technology?	☐ Yes ☐ No ☐ N/A
11. Is a hardened baseline configuration materially rolled out across servers, laptops, desktops and managed mobile devices?	☐ Yes ☐ No ☐ N/A
12. What % of the enterprise is covered by your scheduled vulnerability scans? _____	
13. In what time frame do you install critical and high severity patches across your enterprise? _____	
14. Do you have any end of life or end of support software? *If yes, is it segregated from the rest of the network?*	☐ Yes ☐ No ☐ N/A ☐ Yes ☐ No ☐ N/A
15. Have you configured host-based and network firewalls to disallow inbound connections by default?	☐ Yes ☐ No ☐ N/A
16. Can your users access e-mail through a web app on a non-corporate device? *If yes, do you enforce Multi-Factor Authentication (MFA)?*	☐ Yes ☐ No ☐ N/A ☐ Yes ☐ No ☐ N/A
17. Do you use MFA to protect privileged user accounts?	☐ Yes ☐ No ☐ N/A
18. Do you manage privileged accounts using tooling?	☐ Yes ☐ No ☐ N/A
19. Do your users have local admin rights on their laptop / desktop?	☐ Yes ☐ No ☐ N/A
20. Do you provide your users with a password manager software?	☐ Yes ☐ No ☐ N/A
21. Do you use a protective DNS service?	☐ Yes ☐ No ☐ N/A
22. Do you have a security operations center established? *If yes, is it in-house or outsourced?*	☐ Yes ☐ No ☐ N/A ☐ In-House ☐ Outsourced
23. Are your backups encrypted?	☐ Yes ☐ No ☐ N/A
24. Have you tested the successful restoration and recovery of key server configurations and data from backups in the last six (6) months? *If yes, please detail:* _____	☐ Yes ☐ No ☐ N/A
25. Are your backups kept separate from your network (‘offline’), or in a cloud service designed for this purpose?	☐ Yes ☐ No ☐ N/A
26. Do you use a Cloud syncing service for backups? *If yes, please detail:* _____	☐ Yes ☐ No ☐ N/A

27. Are you able to test the integrity of back-ups prior to restoration to be confident it is free from malware?	☐ Yes ☐ No ☐ N/A

Please describe any additional steps your organization takes to detect and prevent ransomware attacks. Attach to this form on a separate sheet.

PRIOR CLAIMS AND CIRCUMSTANCES

Does the Applicant or other proposed insured (including any director, officer or employee) have knowledge of or information regarding any fact, circumstance, situation, event or transaction which may give rise to a claim, loss or obligation to provide breach notification under the proposed insurance? If yes, please provide details:	☐ Yes ☐ No
During the past five (5) years has the Applicant:	
Received any claims or complaints with respect to privacy, breach of information or network security, unauthorized disclosure of information, or defamation or content infringement?	☐ Yes ☐ No
Been subject to any government action, investigation or subpoena regarding any alleged violation of a privacy law or regulation?	☐ Yes ☐ No
Notified consumers or any other third party of a data breach incident involving the Applicant?	☐ Yes ☐ No
Experienced an actual or attempted extortion demand with respect to its computer systems? If yes, please provide details of any such action, notification, investigation, or subpoena:	☐ Yes ☐ No

SIGNATURE SECTION

The undersigned is authorized by the applicant to sign this application on the applicant's behalf and declares that the statements contained in the information and materials provided to the insurer in conjunction with this application and the undewriting of this insurance are true, accurate and not misleading. Signing of this application does not bind the applicant or the insurer to complete the insurance, but it is agreed that the statements contained in this application and any other information and materials submitted to the insurer in connection with the underwriting of this insurance are the basis of the contract should a policy be issued, and have been relied upon by the insurer in issuing any policy.

This application and all information and materials submitted with it shall be retained on file with the insurer and shall be deemed attached to and become part of the policy if issued. The insurer is authorized to make any investigation and inquiry as it deems necessary regarding the information and materials provided to the insurer in connection with the underwriting and issuance of the policy.

The applicant agrees that if the information provided in this application or in connection with the underwriting of the policy changes between the date of this application and the effective date of the insurance, the applicant will, in order for the information to be accurate on the effective date of the insurance, immediately notify the insurer of such changes, and the insurer may withdraw or modify any outstanding quotations or authorizations or agreements to bind the insurance.

I have read the foregoing application for insurance and represent that the responses provided on behalf of the applicant are true and correct.

FRAUD WARNING DISCLOSURE

Any person who, with intent to defraud or knowing that (s)he is facilitating a fraud against the insurer, submits an application or files a claim containing a false or deceptive statement may be guilty of insurance fraud.

NOTICE TO KANSAS APPLICANT

Any person who, knowingly and with intent to defraud, presents, causes to be presented or prepares with knowledge or belief that it will be presented to or by an insurer, purported insurer, broker or agent thereof, any written, electronic, electronic impulse, facsimile, magnetic, oral, or telephonic communication or statement as part of, or in support of, an application for the issuance of, or the rating of an insurance policy for personal or commercial insurance, or a claim for payment or other benefit pursuant to an insurance policy for commercial or personal insurance which such person knows to contain materially false information concerning any fact material thereto; or conceals, for the purpose of misleading, information concerning any fact material thereto commits a fraudulent insurance act.

Signature: _____ **Date:** _____

Print Name: _____

Title: _____

Please return this application, along with any necessary attachments,
by email to underwriting@kammco.com or by fax to 785.232.4704.

If you work with a KAMMCO agent, please submit this application directly to your agent.