KINGSCOVER
A RISK THEORY COMPANY

CHURCH INSURANCE PROGRAM

Please Send This Completed Form to:
At submission (if not yet quoted): Submissions@KingsCover.com
When bound: Bind@KingsCover.com

CYBER LIABILITY QUESTIONNAIRE (Only Required for limits of $500k+)

Please answer all questions. For Yes/No questions, circle or check the appropriate response. For multi-factor authentication (MFA) questions, N/A is available where applicable - please provide additional explanation for any N/A responses.

REQUEST INFORMATION

Organization Name:

1. Have you, at any time during the past 36 months, experienced a cyber incident (hacking, intrusion, malware infection, fraud loss, breach of personal information, extortion, etc.) that cost you more than $10,000 (in terms of lost business, internal time and labor, external costs, etc.) or experienced a lawsuit or other formal dispute (with either a private party or government agency) arising from a cyber incident? Required

2. Do you collect, process or store more than 250,000 unique personal, health, or credit card information records? Required

3. Does the Applicant (or any other person or organization proposed for this insurance) have knowledge of any act, error, or omission which might give rise to a claim(s) under the proposed policy? If yes, please provide details below.

Details (if yes):

4. Does the Applicant require multi-factor authentication (MFA) for any of the following? (At least one is required):

a. Remote access to the applicant's network Required

b. Access to web-based email Required

c. Access to privileged user accounts Required

** Please provide additional information for any 'N/A' responses to MFA questions above.*

N/A explanation:

5. Does the Applicant back up business-critical data using offline or cloud-based backups on a monthly (or more frequent) basis? Required

6. Does the Applicant verify any change to account details or payment instructions (including ACH payments, account and routing numbers, or wiring instructions) with the requestor via a separate means of communication before implementing any changes? Required

7. Does the Applicant utilize a detection and response system (EDR, MDR, XDR)? Required

8. Does the Applicant utilize a secure email gateway solution (SEG)? Required

9. Does the Applicant require email phishing training for all employees? Required

10. Does the Applicant have a patch management process to test and deploy software patches within thirty (30) days of release? Required