☐ **Navigators Insurance Company**
☐ **Navigators Specialty Insurance Company**

Data Privacy & Security & Media Insurance Application

THIS IS A CLAIMS MADE AND REPORTED POLICY. THIS POLICY APPLIES TO THOSE CLAIMS THAT ARE FIRST MADE AGAINST THE INSURED AND REPORTED IN WRITING TO THE COMPANY DURING THE POLICY PERIOD. CLAIM EXPENSES ARE WITHIN AND REDUCE THE LIMIT OF LIABILITY.

I. General Information

1. Name of Applicant:

   Address: _____

   City: _____ State: _____ Zip: _____

2. Date Established: _____ Website address: _____

3. Please indicate type of Company: ☐ Individual ☐ Partnership ☐ Corporation ☐ Other

4. Is the Applicant owned, controlled, associated or affiliated with any other firm or business enterprise?

   ☐ Yes No ☐ (If yes, please explain including noting whether Applicant shares any computer networks or IT staff with the related entities): _____

5. Please describe the Applicant's business (please attach an additional sheet if necessary): _____

   _____

6. In the past 12 months has the Applicant or any of its principals engaged in any business or profession other than as described in the above question? ☐ Yes ☐ No (If yes, please explain): _____

7. Are there any material changes in the nature or size of the Applicant's business anticipated over the next 12 months? Or have there been any such changes in the past 12 months? ☐ Yes ☐ No

   If yes, please explain: _____

8. Financial Information:

- Fiscal year end date: __/__/_____
- Projected gross revenues for next year: _____
- Gross revenues for current year: _____
- Gross revenues for last year: _____

II. Media Liability

1. Briefly describe steps taken to ensure that the Applicant's published or broadcast content – including domain names, web sites, blogs, and promotional material posted on social media sites – is not infringing or defamatory: _____
2. Do the Applicant's employees or independent contractor make any blog or social media post in the course and scope of their work on behalf of the Applicant? ☐ Yes ☐ No If yes, does the Applicant have a written social media policy that:
   a) Prohibits use of competitor names or trademarks? ☐ Yes ☐ No
   b) Prohibits disclosure of confidential client data? ☐ Yes ☐ No
   c) Prohibits defamatory Comments? ☐ Yes ☐ No
   d) Prohibits or restricts use of company assets for personal posts? ☐ Yes ☐ No
   e) Requires compliance with FTC transparency rules on endorsements? ☐ Yes ☐ No
   f) Governs employee posts related to the company's business or industry? ☐ Yes ☐ No
3. Does the Applicant host any Web content on behalf of or posted by third parties? ☐ Yes ☐ No
   If yes, is there a documented DMCA take down compliance process? ☐ Yes ☐ No
4. Does the Applicant aggregate any content created by others (e.g., news headlines, article synopses, etc.)
   ☐ Yes ☐ No_____

If yes, does the Applicant license this content from its owners? ☐ Yes ☐ No

III. Network Security and Privacy

A. Security and Privacy exposure - Is the Applicant's network used:

1. To access, collect, process, transmit or store credit, debit, bank or brokerage account numbers?

☐ Yes ☐ No

If yes, what is the maximum number stored at any one time? _____

i. Are credit/debit card numbers stored for one time use or repeat use/subscription billing?

☐ One Time Use ☐ Repeat use or subscription billing ☐ N/A – No Card Data Stored

2. To access, collect, process or store social security numbers, medical records or other personal data for non-employees? ☐ Yes ☐ No

If yes, what is the maximum number stored at any one time? _____

3. By third parties who rely on it to access data or process transactions? ☐ Yes ☐ No

4. To access client networks remotely? ☐ Yes ☐ No

5. To provide any web based services including Software as a Service? ☐ Yes ☐ No

6. To generate any revenue from web advertising? ☐ Yes ☐ No

7. To collect information from site visitors, customers or patients that is sold to, or shared with, third parties for marketing purposes? ☐ Yes ☐ No

If yes, please identify methods used to disclose and gain consent:

☐ Terms of Use ☐ Opt-Out provision ☐ Opt-In required

8. To collect any information from site visitors via beacons, HTML cookies, flash cookies, or other tracking software? ☐ Yes ☐ No

If yes, does the Applicant disclose the method(s) used in their terms of use? ☐ Yes ☐ No,

B. Network and Privacy risk controls - does the Applicant:

1. Have company policies:

a) Defining acceptable use of computer assets? ☐Yes ☐ No

b) Limiting web browsing, installation of software? ☐ Yes ☐ No

c) Requiring unique ID's and passwords for all users? ☐ Yes ☐ No

d) Requiring use of strong passwords changed regularly? ☐ Yes ☐ No

2. Have a contractor or trained staff member responsible for information security?

☐ Yes ☐ No

3. Have an employee responsible for privacy compliance & training? ☐ Yes ☐ No

4. Have a written privacy policy for third party data collected and stored on web-site (if applicable), back office systems & paper? ☐ Yes ☐ No

5. Require pre-employment background checks on employees with access to sensitive data?

☐ Yes ☐ No

6. Have a written identity theft prevention program (e.g. to comply with Red Flag rule or similar provisions)?

☐ Yes ☐ No ☐ N/A

7. Conduct annual or more frequent training on security & privacy? ☐ Yes ☐ No

8. Change default passwords on firewalls, routers & other security appliances?

☐ Yes ☐ No

9. Use Anti-Virus software with automatic update? ☐ Yes ☐ No

10. Annually re-assess security practices? ☐ Yes ☐ No

11. Use automatic security patch updates when available from software vendors and install critical security patches within 120 days? ☐ Yes ☐ No

12. Filter web and email content for executable files, prohibited sites, spam, etc? ☐ Yes ☐ No

13. Employ change control to ensure that systems modifications do not compromise network security?

☐ Yes ☐ No

14. Set access privileges that grant the least level of privilege necessary for users and programs to complete assigned functions? ☐ Yes ☐ No

15. Restrict network administrative privileges for most users? ☐ Yes ☐ No

16. Delete access within 48 hours of termination? ☐ Yes ☐ No

17. Conduct audits of authorized user access to sensitive data? ☐ Yes ☐ No

18. Encrypt:

a) Databases? ☐ Yes ☐ No

b) Sensitive data on laptops/mobile devices ☐ Yes ☐ No ☐ N/A

c) Sensitive data stored in cloud environments (any servers not in the Applicant's direct control)?

☐ Yes ☐ No ☐ N/A

d) Back-up tapes, flash drives, and other portable storage media? ☐ Yes ☐ No

e) In transit within the network? ☐ Yes ☐ No

f) In transit over public networks ☐ Yes ☐ No

19. Employ physical security for premises, computer rooms, etc.? ☐ Yes ☐ No

20. Conduct annual or more frequent vulnerability scans? ☐ Yes ☐ No

21. Use intrusion prevention and detection systems? ☐ Yes ☐ No

22. Monitor event logs for network, remote connections and databases housing sensitive data?

☐ Yes ☐ No

23. Use egress filtering and/or other Data Loss Prevention systems? ☐ Yes ☐ No

24. Ensure permanent destruction of sensitive data before files or devices are disposed of? ☐ Yes ☐ No

25. Limit remote access only via VPN or other secure means? ☐ Yes ☐ No ☐ N/A

26. Require two-factor authentication for remote access? ☐ Yes ☐ No ☐ N/A

27. Employ WPA/WPA2 or more recent standard (i.e., not WEP) for all wireless access?

☐ Yes ☐ No ☐ N/A

28. Masked, encrypt and purge credit/debit card numbers in compliance with PCI standards?

☐ Yes ☐ No ☐ N/A

29. Prevent storage of card security code (CSC/CVV) values? ☐ Yes ☐ No ☐N/A

30. Verify PCI and/or HIPAA Compliance by audit? ☐ Yes ☐ No ☐ N/A

31. Limit collection and viewing of sensitive information on web site to secure web pages?

☐ Yes ☐ No ☐ N/A

32. Require web applications – whether developed by insured or vendors – are hardened against know web attacks (e.g., SQL injection, cross Scripting, etc.)? ☐ Yes ☐ No ☐ N/A

33. Contractually require vendors to whom sensitive data is entrusted or which have access to insured are network contractually required to protect data? ☐ Yes ☐ No ☐ N/A

34. Contractually require vendors to whom sensitive data is entrusted or which have access to insured's network contractually required to indemnify insured? ☐ Yes ☐ No ☐ N/A

35. Have a disaster recovery plan? ☐ Yes ☐ No

36. Have an Incident response plan for privacy breaches that is test annually? ☐ Yes ☐ No

37. Shred paper records with sensitive information prior to disposal? ☐ Yes ☐ No

38. Ensure that sensitive data is permanently removed from computers and other electronic storage media prior to recycling, donation, re-sale, or disposal? ☐ Yes ☐ No

IV Historical Information

1. Prior Data Privacy & Security/Media Insurance:

Year	Insurance Company	Limit of Liability	Deductible	Premium	Claims Made or Occurrence Policy Form	Policy Period	Retroactive Date (if any)
Current Year							
Previous Year 1							
Previous Year 2							
Previous Year 3							

Previous Year 4							

2. Is any Extended Reporting Period (ERP) currently in place? ☐ Yes ☐ No (If yes, please attach a copy of the endorsement including effective and expiration date).

3. Has any Data Privacy & Security/Media insurance ever been declined or cancelled?

   If yes, explain: _____

4. Has the Applicant been a party to any lawsuit or other legal proceeding within the past five years?

   ☐ Yes ☐ No

   If yes, please attach a supplemental claims questionnaire or provide a detailed description which includes the parties involved, the amount at dispute, the nature of the claim(s), the status of the action(s) and how the action(s) was resolved as to the applicant, including all costs incurred; including defense expenses.

5. After inquiry, have any media, data privacy breach or network compromise claims been made during the past five years against the Applicant or any past or present principals, partners, directors, officers or professional employees?

   ☐ Yes ☐ No (If yes, please complete a supplemental claims questionnaire)

6. After inquiry, does the Applicant or any principal, partner, director, officer or professional employee have any knowledge or information of any act, error, omission, data privacy breach, network compromise fact, or circumstance which may give rise to a claim being made against them?

   ☐ Yes ☐ No (If yes, please complete a supplemental claims questionnaire).

Please provide the following additional information:

1. **Latest financial statements and company literature (if there is no company website).**
2. **Copy of most recent internal or third party network security audit**

Applicant hereby represents after inquiry, that information contained herein and in any supplemental applications or forms required hereby, is true, accurate and complete, and that no material facts have been suppressed or misstated. Applicant acknowledges a continuing obligation to report to the Company as soon as practicable any material changes in all such information, after signing the application and prior to issuance of the policy, and acknowledges that the Company shall have the right to withdraw or modify any outstanding quotations and/or authorization or agreement to bind the insurance based upon such changes.

Further, Applicant understands and acknowledges that:

1. If a policy is issued, the Company will have relied upon, as representations, this application, any supplemental applications, and any other statements furnished to the Company in conjunction with this application, all of which are hereby incorporated by reference into this application and made a part thereof
2. This application will be the basis of the contract and will be incorporated by references into and made part of such policy; and
3. Applicant's failure to report to its current insurance company any claim made against it during the current policy term, or act, omission or circumstances which Applicant is aware of which may give rise to a claim before the expiration of the current policy may create a lack of coverage for each Applicant who had a basis to believe that any such act, error, omission or circumstance might reasonably be expected to be the basis of a claim.
4. The policy applied for provides coverage on a claims made and reported basis and will apply only to claims that are first made against the insured and reported in writing to the Company during the policy period. Claims expenses are within and reduce the limit of liability.

NOTICE: IN CERTAIN STATES, ANY PERSON WHO KNOWINGLY AND WITH INTENT TO DEFRAUD ANY INSURANCE COMPANY OR OTHER PERSON FILES AN APPLICATION FOR INSURANCE CONTAINING ANY FALSE INFORMATION, OR CONCEALS FOR THE PURPOSE OF MISLEADING INFORMATION CONCERNING ANY FACT MATERIAL THERETO, COMMITS A FRAUDULENT INSURANCE ACT, WHICH IS A CRIME.

Applicant: Title:

Applicant's Signature: Date:

Agent/Broker Name: