

Network Security & Privacy Supplemental Application

WITH NAVIGATORS INSURANCE COMPANY OR
NAVIGATORS SPECIALTY INSURANCE COMPANY

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. Basic 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):

II. Network Security and Privacy

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

1. To store credit, debit, bank or brokerage account numbers? Yes No

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

< 3,000 3,001-20,000 > 20,000

2. To 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?

<10,000 10,001-50,000 >50,000

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

4. To access client networks remotely? Yes No

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

1. Have company policy:

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

2. Requiring use of strong passwords changed regularly? Yes No

3. Have a contractor or trained staff member responsible for information security?
 Yes No

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

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

6. Require pre-employment background checks on employees with access to sensitive data?
 Yes No

7. Have a written identity theft prevention program (e.g. to comply with Red Flag rule or similar provisions)? Yes No N/A

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

9. Change default passwords on firewalls, routers & other security appliances?
 Yes No

10. Use Anti-Virus software with automatic update? Yes No
11. Annually re-assess security practices? Yes No
12. Use automatic security patch updates when available from software vendors and install critical security patches within 120 days? Yes No
13. Filter web and email content for executable files, prohibited sites, spam, etc? Yes No
14. Employ change control to ensure that systems modifications do not compromise network security?
 Yes No
15. Set access privileges that grant the least level of privilege necessary for users and programs to complete assigned functions? Yes No
16. Restrict network administrative privileges for most users? Yes No
17. Delete access within 48 hours of termination? Yes No
18. Conduct audits of authorized user access to sensitive data? Yes No
19. Encrypt:
- a. Databases? Yes No
 - b. Sensitive data on laptops/mobile devices Yes No N/A
 - c. Back-up tapes, flash drives, and other portable storage media? Yes No
 - d. In transit within the network? Yes No
 - e. In transit over public networks Yes No
20. Employ physical security for premises, computer rooms, etc.? Yes No
21. Conduct annual or more frequent vulnerability scans? Yes No
22. Use intrusion prevention and detection systems? Yes No
23. Monitor event logs for network, remote connections and databases housing sensitive data?
 Yes No
24. Use egress filtering and/or other Data Loss Prevention systems? Yes No
25. Ensure permanent destruction of sensitive data before files or devices are disposed of? Yes No

26. Limit remote access only via VPN or other secure means? Yes No N/A
27. Require two factor authentication for remote access? Yes No N/A
28. Employ WPA/WPA2 or more recent standard (i.e., not WEP) for all wireless access?
 Yes No N/A
29. Masked, encrypt and purge Credit/debit card numbers in compliance with PCI standards?
 Yes No N/A
30. Prevent storage of card security code (CSC/CVV) values? Yes No N/A
31. Verify PCI and/or HIPAA Compliance by audit? Yes No N/A
32. Limit collection and viewing of sensitive information to secure web pages?
 Yes No N/A
33. 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
34. 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
35. 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
36. Have a disaster recovery plan? Yes No
37. Have an Incident response plan for privacy breaches? Yes No

III. Historical Information

1. Has the Applicant been a party to any lawsuit or other legal proceeding regarding an actual or alleged data privacy breach or network compromise 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.

2. After inquiry, have any 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).

3. After inquiry, does the Applicant or any principal, partner, director, officer or professional employee have any knowledge or information of any data privacy breach or 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. Copy of most recent internal or third party network security audit (if applicable)

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: _____