



Application for Insurance The Data Risk Containment Program



THE COVERAGE AFFORDED BY THIS POLICY IS LIMITED TO LIABILITY FOR THOSE **CLAIMS** FIRST MADE AGAINST AN **INSURED** DURING THE **POLICY PERIOD** OR THOSE **DATA CONTAINMENT EVENTS** WHICH **YOU** FIRST LEARN OF DURING THE **POLICY PERIOD**, AS SET FORTH IN THE POLICY.

General Information:

1. Name of the Applicant: _____
Address: _____
City/State/Zip: _____
County: _____

2. Website Address: _____

3. Define the company Class of Business (if multiple, then as a percentage of revenues):

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):

4. Please indicate type of Company: Individual Partnership Corporation Other

5. How long has the company been in business? _____

6. Is your company regulated by any of the following?:

- HIPAA/HITECH: Yes No
- Graham-Leach Bliley: Yes No
- FACTA/Red Flag Rules: Yes No
- PCI: Yes No
- Sarbanes-Oxley: Yes No

7. Is the company compliant with any regulations required above?

Yes No

8. Is the company appropriately licensed and/or authorized as required to transact business in the state of domicile?

Yes No

9. How many records (personally identifiable information (PII) or protected health information (PHI)) is the company responsible for? _____

10. Does the company currently purchase a form of "cyber" liability or data security insurance? If so:

- Carrier: _____
- Limit/Self Insured Retention: _____
- Premium: _____
- Retroactive Date: _____

11. What limit and self-insured retention amount is the company requesting? _____



12. Is the company currently involved in any litigation with a federal agency, including the Federal Trade Commission or applicable state or local agencies? Yes No (If yes, please explain): _____

13. Is the company currently under protection of a U.S. Bankruptcy Judge or Trustee? Yes No (If yes, please explain): _____

14. Has the Applicant been a party to any lawsuit or other legal proceeding within the past five years? Yes No
If yes, please attach 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.
15. After inquiry, has a data privacy breach or network compromise claim 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 explain)

16. 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 explain)

17. Financial Information:
- o When does your fiscal year end? _____
 - o What were your company's revenues during the last fiscal year? _____
 - o What are your revenue projections for this fiscal year? _____
 - o Do current assets exceed current liabilities? _____

Security Culture:

1. Is any component of Information Technology/Information Security outsourced?
 Yes No (If yes, please explain): _____
2. Is all Sensitive Information, for which the company is responsible, stored separately from non-sensitive information?
 Yes No
3. Does the company have a defined information security team with documented duties and responsibilities? Yes No
4. Are all employees periodically trained and tested on the policies and procedures for protecting PII / PHI prior to having access to such information? Yes No
5. Are all employees trained and tested at least annually on their knowledge of security procedures and emerging threats such that the employees can recognize the early signs of such attacks and promptly report them? Yes No



6. What is the frequency of the training? _____
7. Are written policies and procedures in place for tracking software patches and updates including dates announced and date installed? Yes No
8. How are software patches tracked? [Manual / Paper based or Electronic]
9. Do you have policies and procedures enforcing strong passwords? Yes No
10. Are technology safeguards in place that force strong passwords to be changed on a regularly scheduled basis? Yes No
11. Are technology safeguards in place that prevent password reuse? Yes No
12. Are procedures or systems in place to prevent clear text transmission of passwords, including through email or instant messaging? Yes No
13. Are vulnerability scans or penetration tests performed at least annually on critical systems inside the company network?
 Yes No (If No, may we perform a vulnerability scan on the network?) _____
14. Which term best describes your IT department's approach to date security ? Proactive Reactive

Security Configuration:

1. How many demarcation (DEMARCO) points does the company have? _____
2. How many remote locations does the company have? _____
3. Are procedures and systems in place to log and issue a warning if a privileged access account is accessed? Yes No
4. Are the company's operating systems, programs and operating information backed up, as well as data? Yes No
5. Where are the backups stored? On-Site Off-Site
6. Are the backups encrypted? Yes No
7. Is internally stored PII or PHI information accessed by systems different from the ones that handle web transactions?
 Yes No
8. Does you company have wireless network capability? Yes No
9. If yes above, is access encrypted with at least WPA or WPA2? Yes No
10. Are all portable laptops, media, flash drives encrypted? Yes No
11. Are policies and procedures in place defining security requirements for portable digital assistants (PDAs) smart phones, USB drives, and other devises that could be connected to the network? Yes No
12. Does the company filter out executable e-mail attachments? Yes No
13. Are intrusion detection (IDS) or intrusion prevention systems (IPS) used on the network? Yes No
14. What is your policy for reviewing the logs from IDS and IPS systems? _____
15. What brand(s) of Firewall does the company use? _____
16. Are policies for firewalls, IDS and IPS systems reviewed on a regular basis? Yes No
17. Is the network regularly scanned for unauthorized systems? Yes No

Vendor Management/Contractual Governance:

1. Is any company or client sensitive information stored in "the cloud"? Yes No



2. Are all third party vendors who may have access to any sensitive company or client information required to demonstrate adequate security policies, procedures and systems? Yes No
3. Are all vendors who may have access to sensitive company or client information required to provide contractual indemnification for harm arising out of a data exposure? Yes No
4. Are these vendors required to carry adequate limit of insurance, specific to the data exposure risk and their indemnification obligation? Yes No
5. Does the company provide any professional services for which it has agreed contractually to provide indemnification for harm arising from a data breach? Yes No
6. Describe how the company manages disposal or destruction of PII/PHI?

Please provide the following additional information:

1. **A specimen copy of any contracts providing data security indemnification to clients and/or from vendors.**
2. **Copy of the last two internal or third party network security audits, along with recommendations**

Applicant hereby represents after inquiry, that any information contained herein are true, accurate and complete, and that no material facts have been suppressed or misstated. Further, Applicant understands and acknowledges that:

1. If a policy is issued, the **We** will have relied upon, as representations, this application and any other statements furnished to **Us** 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.

NOTICE: Applicants are underwritten by US Risk Underwriters. RiskAnalytics makes no warranty or representations, expressed or implied, with regard to the integrity of accuracy of the information contained within this application.

I hereby certify that I have read and understand the items on this application and that my answers are true and complete to the best of my knowledge.

Signed: _____

Must be signed by an officer of the Company who is authorized to sign on Applicant's behalf.

Date: _____

Agent/Broker's Name: _____

Please return completed application form and any attachments to bbranner@riskanalytics.com, or via fax number 913.685.9401.