Putting risk in its place

BrP BusinessRisk PARTNERS

2 Waterside Crossing, Suite 102, Windsor, CT 06095
phone 860.903.0000 *fax* 860.903.0001
www.businessriskpartners.com

CYBER SUPPLEMENTAL APPLICATION

I. General Information

1. Name of Applicant:

2. Type of Information the Applicant collects, processes or stores (check all that apply):

   Social Security Numbers □
   Credit Card Information □
   Employee Information □
   Intellectual Property Assets □
   Personal Health Information □
   Bank Account Information □
   Money/Securities Information □
   Other:

3. Estimated number of unique records stored by the Applicant:

II. Information Security & Content Controls

4. Does the Applicant's website include a privacy policy or terms of use agreement? □ Yes □ No

5. Do the Applicant's website(s) or social media site(s) allow for users to post content? □ Yes □ No
   If Yes, does the Applicant have guidelines in place to remove offensive or infringing content? □ Yes □ No

6. Does the Applicant's media clearance and compliance procedures include:
   a. measures to ensure acquisition of all necessary intellectual property (IP) rights and publicity rights of all content through releases, licenses or consents? □ Yes □ No
   b. standard procedures to handle complaints concerning disseminated material? □ Yes □ No
   c. training of employees regarding copyright and trademark issues? □ Yes □ No

7. Does the Applicant have a designated person or group within the organization responsible for all network security and privacy-related matters? □ Yes □ No

8. Does the Applicant maintain the following corporate-wide policies:

	Check if Yes*	Reviewed by Attorney?	Frequency of Updates (daily, monthly, yearly, etc)
Information Security and Privacy Policy	□	□ Y □ N	
Business Continuity and Disaster Recovery Plan	□	□ Y □ N	
Information Security Incident Response Plan	□	□ Y □ N	
Document Retention And Destruction Policy	□	□ Y □ N	

9. If the Applicant processes, stores, or handles credit card transactions, is it compliant with Payment Card Industry Data Security Standards (PCI DSS)? □ Yes □ No □ N/A
   If Yes, please indicate the required level of compliance: □ 1 □ 2 □ 3 □ 4

10. Check all services that are outsourced by the Applicant and indicate the name of the vendor providing the service:
    □ Data Center Hosting:
    □ Data Processing:
    □ Application Service Provider:
    □ Managed Security:
    □ Alert Log Monitoring:
    □ Intrusion Detection:

11. Does the Applicant require all vendors to whom services are outsourced to hold the Applicant harmless for a breach at the vendor's organization? □ Yes □ No □ N/A

12. In the event of a computer attack or other loss/ corruption of data, how long does it take the Applicant to restore operations?
□ 12 hours or less □ 12 to 24 hours □ more than 24 hours □Not known

13. With regard to the Applicant's organization, including its network, websites and portable devices, does the Applicant:
    a. utilize encryption tools to enhance the integrity of confidential Information? □ Yes □ No
    If Yes, is encryption utilized for data: □ At rest □ In Transit □ On backup media □ On portable devices
    b. grant access to confidential Information on a least privileged access basis? □ Yes □ No
    c. utilize strong password requirements for access to confidential Information? □ Yes □ No
    d. have physical security controls in place to limit access to confidential Information? □ Yes □ No
    e. backup sensitive data on a regular basis? □ Yes □ No
    If Yes, how often? □ hourly □ daily □ weekly □ monthly □ other:
    f. utilize intrusion detection or data loss prevention tools to monitor its networks? □ Yes □ No
    g. employ firewalls on all network components that process or store confidential Information? □ Yes □ No
    h. conduct data security and privacy training for all employees? □ Yes □ No
    i. conduct any information security or privacy assessment regularly to ensure compliance with any specific privacy requirements that govern its industry(ies)? □ Yes □ No
    j. conduct regular penetration testing or vulnerability scans of their computer systems? □ Yes □ No

14. If the Applicant answered "Yes" to 13.i. or 13.j. above,:
    a. were any weaknesses or vulnerabilities detected? □ Yes □ No □ N/A
    b. were all identified weaknesses and/ or vulnerabilities remediated immediately? □ Yes □ No □ N/A

If No to any question in #13 or #14 above, please explain:

III. Claim History

15. Is the applicant or any of its former or current directors, officers, employees, subsidiaries or independent contractors aware of any circumstances or occurrences , claims or losses related to: a failure of security of the Applicant's computer system; an invasion or interference with rights of privacy or wrongful disclosure of confidential Information, or an act, error, omission, breach of duty, cease and desist letter, alleged breach of intellectual property rights, or any other circumstance which may reasonably result in a claim relative to the insurance sought? □ Yes □ No

If Yes, please provide a detailed description of the facts or circumstances, the status of the action(s), and any costs incurred to date (use a separate sheet if necessary):

IV. DECLARATION AND SIGNATURE

The undersigned is a duly authorized representative of the Applicant identified in answer to Question No. 1 herein and acknowledges that reasonable inquiry has been made to obtain the answers to all of the questions herein and the information and documents submitted herewith, all of which are true, accurate and complete to the best of the undersigned's knowledge and belief.

Signed: ____

Title: ____
(This application must be signed by a duly authorized representative of the Applicant)

Company: ____

Date: ____