OneBeacon
PROFESSIONAL INSURANCE®

6800 College Blvd., Suite 350
Overland Park, KS 66211
913-384-4800 • 800-753-7545 • Fax: 913-384-4822
www.onebeaconpro.com

Website and Data Security Questionnaire

General Security/Confidentiality Practices

1. Does the Applicant employ a Chief Information Officer? ☐ Yes ☐ No
2. Does the Applicant employ a Chief Security Officer? ☐ Yes ☐ No
3. Do the above positions report to the Board of Directors? ☐ Yes ☐ No

4. Does the Applicant have a corporate-wide privacy policy? ☐ Yes ☐ No
5. Have the Applicant's privacy policies been reviewed and approved by an attorney? ☐ Yes ☐ No

6. How often are the company's policies reviewed and updated? _____

7. Does the Applicant maintain formal employee on-boarding and off-boarding procedures? ☐ Yes ☐ No
8. Does the Applicant have restricted employee access to private information? ☐ Yes ☐ No
9. Does the Applicant have internal training for employees concerning the handling of data security and private, personal, and sensitive information? ☐ Yes ☐ No

10. Are employee background checks, including criminal background, completed on employees who will have access to Personally Identifiable Information? ☐ Yes ☐ No

11. In the past twenty-four (24) months, has the Applicant undergone an internal or external privacy or network security audit or assessment? ☐ Yes ☐ No

12. Have all recommendations been implemented? ☐ Yes ☐ No

    If No, please explain:

    _____

13. Does the Applicant collect, receive, process, transmit, or maintain private, sensitive, or personal information as part of its business activities? ☐ Yes ☐ No

    If Yes, please indicate what type:

☐	Credit/Debit Card Data	☐	Medical Records
☐	Social Security Numbers	☐	Employee/HR Information
☐	Bank Accounts and Records	☐	Intellectual property of others
☐	Customer Information	☐	Medical Information
☐	Confidentiality Agreements	☐	Trade Secrets
☐	Other: _____		

    Personally Identifiable Information:

    Approximate number of individual records stored on **Applicant's** network: _____

    i. Is any of this information regulated by HIPAA, GLB, the Data Protection Act or any other law or regulation protecting private, sensitive, or personal information? ☐ Yes ☐ No

ii. Does the Applicant have written procedures in place to comply with laws governing the handling or disclosure of such information, including any Red Flag Rules? ☐ Yes ☐ No

iii. Does the Applicant share private, sensitive, or personal information gathered from customers (by the Applicant or others) with third parties? ☐ Yes ☐ No

iii. If Yes to the above question (iii), is permission obtained? ☐ Yes ☐ No

14. Does the Applicant have a vendor approval process? ☐ Yes ☐ No
15. Does the Applicant require vendors to carry professional liability insurance? ☐ Yes ☐ No

16. Does the Applicant require a written contract with all vendors? ☐ Yes ☐ No
    a. If Yes, are all contract reviewed by the internal legal department or an outside law firm? ☐ Yes ☐ No

17. Does the Applicant require that contracts with outside companies and vendors necessitate those companies to defend and indemnify the Applicant in the event there is any loss arising out of the release or disclosure of private, sensitive, or personal information due to the outside company or vendor's negligence? ☐ Yes ☐ No

IV. NETWORK SECURITY INFORMATION

1. Does the Applicant have a written and tested:

    a. Disaster Recovery Plan? ☐ Yes ☐ No
    b. Business Continuity Plan? ☐ Yes ☐ No
    c. Data Loss Prevention Plan? ☐ Yes ☐ No
    d. Computer security policy? ☐ Yes ☐ No
    e. Procedure to change default credentials? ☐ Yes ☐ No
    f. Laptop security policy? ☐ Yes ☐ No
    g. Removable Media/USB Policy? ☐ Yes ☐ No
    h. Remote Access Policy? ☐ Yes ☐ No
    i. Mobile Device/Smartphone Policy? ☐ Yes ☐ No
    j. Breach Disclosure Policy? ☐ Yes ☐ No

2. Does the Applicant store sensitive data on web servers? ☐ Yes ☐ No

    a. If Yes, is the data encrypted? ☐ Yes ☐ No
    b. If No, please describe any offsetting measures:

    _____

3. Is the Applicant's data that is both "at-rest" and "in-transit" encrypted? ☐ Yes ☐ No

4. Does the Applicant store personally identifiable or other confidential information on laptops, smart phones, memory sticks or other mobile devices? ☐ Yes ☐ No

    a. If Yes, does the Applicant encrypt such information? ☐ Yes ☐ No

5. Does the Applicant use third-party technology service providers? ☐ Yes ☐ No
    a. If Yes, what services does the Applicant utilize:

        i. Hosting of Applicant's network: ☐ Yes ☐ No
        ii. Maintenance: ☐ Yes ☐ No
        iii. Website hosting: ☐ Yes ☐ No
        iv. Storage and back-up of electronic data: ☐ Yes ☐ No
        v. Storage and back-up of sensitive data: ☐ Yes ☐ No
        vi. Other: _____

6. Do network administrators maintain separate accounts for administration purposes from the accounts they use for general network connectivity? ☐ Yes ☐ No

7. Does the Applicant use security and firewall technology? ☐ Yes ☐ No

8. Does the Applicant host services directly accessible from the public internet? ☐ Yes ☐ No
   a. If Yes, please indicate what services:
      i. E-Commerce ☐ Yes ☐ No
      ii. Customer Portal ☐ Yes ☐ No
      iii. Dynamic Data (inventory, quote, etc.) ☐ Yes ☐ No
      iv. General Information ☐ Yes ☐ No
      v. Other: _____

   b. If Yes to above, are the publically accessible servers segmented from the internal LAN with a firewall? ☐ Yes ☐ No

9. Are border firewall configured to restrict outbound connections (egress filtering) to only Business related services? ☐ Yes ☐ No

10. Is it the Applicant's policy to up-grade all security software as new releases/improvements become available? ☐ Yes ☐ No

11. Is a patch management solution in place? ☐ Yes ☐ No

    a. Is the patch management solution capable of patching Microsoft as well as third-party application? ☐ Yes ☐ No

12. Is there a managed anti-virus solution in place? ☐ Yes ☐ No

    a. Is anti-virus software installed on all of the Applicant's computer systems, including laptops, personal computers, and networks? ☐ Yes ☐ No

    b. How often are updates applied? _____

13. Does the Applicant use intrusion detection software to detect unauthorized access to internal networks and computer systems? ☐ Yes ☐ No

14. Does the Applicant have a formal documented user and password procedure in place? ☐ Yes ☐ No

15. Does the Applicant limit access to network servers and hardware? ☐ Yes ☐ No

16. Are all servers located in a physically secure location? ☐ Yes ☐ No

17. Is physical access to the servers logged? ☐ Yes ☐ No

18. Is physical access to the servers monitored with video surveillance? ☐ Yes ☐ No

19. Does the Applicant provide remote access to its network? ☐ Yes ☐ No
    a. Is remote access restricted to Virtual Private Networks (VPNs)? ☐ Yes ☐ No

20. Does remote access connectivity to the network require two-factor authentication? ☐ Yes ☐ No

21. Are remote access connections logged? ☐ Yes ☐ No

22. Are user accounts automatically locked out after a specified number of invalid logon attempts? ☐ Yes ☐ No

a. How many failed attempts? _____
b. How long before the account is locked out? _____

23. Is wireless network connectivity available? ☐ Yes ☐ No

a. What security requirements are employed?
   i. WEP ☐
   ii. WPA - PSK (Pre-Shared Key or password-based authentication) ☐
   iii. WPA – EAP (Extensible Authentication Protocol or user-based authentication) ☐

24. How often is private/personal/sensitive/valuable information archived? _____

a. How long is the information stored? _____
b. Is the information stored in an off-premises secondary site ☐ Yes ☐ No

25. Does the Applicant terminate all associated computer access and user accounts when an employee leaves the company? ☐ Yes ☐ No

26. Are the Applicant's internal networks and computer systems subject to third party audit and monitoring? ☐ Yes ☐ No

a. If Yes, when was the last audit? _____
b. Have all improvements and recommendations been implemented? ☐ Yes ☐ No
c. If No, please explain: _____

27. Does the Applicant have a secondary site available if the primary site becomes inoperative? ☐ Yes ☐ No

28. How long before the second site becomes operational? _____

29. Is the Applicant Payment Card Industry (PCI) Data Security Standard compliant? ☐ Yes ☐ No

a. If Yes, please select level of compliance: ☐ 1 ☐ 2 ☐ 3 ☐ 4

Loss History and Other Information

1. Has the Applicant suffered any known intrusions, unauthorized access, or been a target of a security or virus incident of its computer systems? ☐ Yes ☐ No

i. If Yes, how many intrusions occurred? _____

If any damage was caused by any such intrusions, including lost time, lost business income, or costs to repair any damage to systems or to reconstruct data or software, describe the damage that occurred, and state value of any lost time, income and the costs of any repair or reconstruction:

_____

_____

2. After inquiry does any principal, partner, director or officer or professional employee have knowledge or information of any circumstance or any allegation or contentions of any incident which may result in any claim being made against them for any network security incident, right to privacy, disclosure of personal information, or any violation of any related privacy statute or regulation? ☐ Yes ☐ No

If Yes, please explain:

Additional Answer/Comments to the above Questions

Signature of Applicant: _____ Date: _____