Business Privacy and Information Security Questionnaire

Following are forty (40) questions to assess your Firm's information privacy posture.

1. Does the Business define and document its privacy and information security policies?
   [ ] Yes
   [ ] No
   [ ] Maybe
   Comment: _____

2. Are privacy and information security policies and the consequences of noncompliance with such policies are communicated, at least annually, to the business's internal personnel responsible for collecting, using, retaining, and disclosing personal information?
   [ ] Yes
   [ ] No
   [ ] Maybe
   Comment: _____

3. Are changes in privacy and information security policies are communicated to such personnel shortly after the changes are approved?
   [ ] Yes
   [ ] No
   [ ] Maybe
   Comment: _____

4. Is responsibility and accountability assigned to a person or group for developing, documenting, implementing, enforcing,

monitoring,and updating the business's privacy and information security policies?
[ ] Yes
[ ] No
[ ] Maybe
Comment: _____

5. Are privacy and information security policies and procedures, and changes thereto, reviewed and approved by the business's management?
[ ] Yes
[ ] No
[ ] Maybe
Comment: _____

6. Does the firm have a written third party risk management program that it actively staffs and uses to assess, at least annually, the effectiveness of third party privacy and information security policies, procedures and contracts to protect sensitive personal information shared by the business with those third parties?
[ ] Yes
[ ] No
[ ] Maybe
Comment: _____

7. Has the firm created and does the firm actively maintain maps of the systems, storage and flow of sensitive nonpublic information, including NPI, corporate proprietary and third party protected information and use those maps to manage and communicate about the business's privacy and information security program?
[ ] Yes
[ ] No
[ ] Maybe
Comment: _____

8. Do internal personnel or advisers review contracts for consistency with privacy and information security policies and procedures, assign responsibilities and liability for data breaches and address any inconsistencies?
   [ ] Yes
   [ ] No
   [ ] Maybe
   Comment: _____

9. Is the potential privacy and information security impact assessed when new processes involving personal information are implemented, whether they are internal or performed by a third party? (For this purpose, "processes" involving personal information include the design, acquisition, development, implementation, configuration, modification and management of the following: (i) Infrastructure, (ii) Systems, (iii) Applications, (iv) Web sites, (v) Procedures, (vi) Products and Services, (vii)Data bases and (viii) Mobile computing)

[ ] Yes
[ ] No
[ ] Maybe
Comment: _____

10. Has a documented privacy and information security incident and breach management program been implemented and tested at least annually?
    [ ] Yes
    [ ] No
    [ ] Maybe
    Comment: _____

11. Is the business prepared to communicate to employees, clients, and the media during a data loss incident?

[ ] Yes
[ ] No
[ ] Maybe
Comment: _____

12. Has the business established qualifications for personnel responsible for protecting the privacy and security of personal information and assigned such responsibilities only to those personnel who meet these qualifications and have received needed training?
[ ] Yes
[ ] No
[ ] Maybe
Comment: _____

13. Is privacy training provided to each and every employee regardless of position with addition training provided for employees handling extremely sensitive information? Does this training including intentional phishing of employees to identify employees in need of additional training? Does this training occur on a continuing basis rather than at some fixed frequency such as annually? Note: only answer yes to this question of all parts can be answered yes; otherwise, answer no and explain in the comments
[ ] Yes
[ ] No
[ ] Maybe
Comment: _____

14. For each legal jurisdiction in which the business operates, is the effect of jurisdiction-specific privacy requirements identified and addressed? Note: this may include locations that firm is licensed in but has no physical presence and locations that the firm targets marketing to via online services or advertising materials.

[ ] Yes
[ ] No
[ ] Maybe
Comment: _____

15. Do the business's privacy policies address the protection, use, retention, and disposal of Client information?
[ ] Yes
[ ] No
[ ] Maybe
Comment: _____

16. Is confidential information that is no longer retained anonymized, disposed of, or destroyed in a manner that prevents loss, theft, misuse, or unauthorized access?
[ ] Yes
[ ] No
[ ] Maybe
Comment: _____

17. Does the business's privacy policies address the disclosure of personal information to third parties?
[ ] Yes
[ ] No
[ ] Maybe
Comment: _____

18. Do the Law Firm's privacy policies (including any relevant security policies) address the security of confidential information?

[ ] Yes
[ ] No
[ ] Maybe
Comment: _____

19. Has a security program been developed, documented, approved, and implemented that includes administrative, technical, and physical safeguards to protect personal information from loss, misuse, unauthorized access, disclosure, alteration, and/or destruction?

[ ] Yes
[ ] No
[ ] Maybe
Comment: _____

20. Does the IT Security Program address, the following areas related to the security of personal information: (i) Risk assessment and treatment, (ii) Security policies, (iii) Human resources security, (iv) Physical and environmental security, (v) Access control, (vi) Business continuity management and (vii) Compliance?

[ ] Yes
[ ] No
[ ] Maybe
Comment: _____

21. Is Logical access to confidential information restricted by procedures that address limiting access to such information to only authorized internal personnel based upon their assigned roles and responsibilities.

[ ] Yes
[ ] No
[ ] Maybe
Comment: _____

22. Is confidential information, in all forms, protected against accidental disclosure due to natural disasters and environmental hazards?

[ ] Yes
[ ] No
[ ] Maybe
Comment: _____

23. Is confidential information collected and transmitted over the Internet, over public and other non-secure networks, and wireless networks protected by deploying industry standard encryption technology for transferring and receiving personal information?

[ ] Yes
[ ] No
[ ] Maybe
Comment: _____

24. Is confidential information stored on portable media or devices is protected from unauthorized access?

[ ] Yes
[ ] No
[ ] Maybe
Comment: _____

25. Are tests of the effectiveness of the key administrative, technical, and physical safeguards protecting personal information conducted at least annually by an independent firm with cyber security expertise?

[ ] Yes
[ ] No
[ ] Maybe

Comment: _____

26. Do the Law Firm's privacy policies address the monitoring and enforcement of privacy policies and procedures?

[ ] Yes
[ ] No
[ ] Maybe
Comment: _____

27. Are ongoing procedures performed for monitoring the effectiveness of controls over confidential information, based on a risk assessment, and for taking timely corrective actions where necessary?

[ ] Yes
[ ] No
[ ] Maybe
Comment: _____

28. Has the business compared its policies and procedures with the Federal Trade Commission's report on "Protecting Personal Information: A Guide for Business"?

[ ] Yes
[ ] No
[ ] Maybe

Comment: _____

29. Has the business compared its Cybersecurity practices against the Federal Trade Commission's practical guidance on how to reduce Cybersecurity risks?

[ ] Yes
[ ] No
[ ] Maybe
Comment: _____

30. Forty-five states and the District of Columbia require notification of security breaches involving personal information, and in some states the law outlines the information that must be included in the notification. Does the business have a data breach notification policy in compliance with the requirements of these various jurisdictions?

[ ] Yes
[ ] No
[ ] Maybe
Comment: _____

31. Does the business allow employees to connect their personal devices on the entity's network?

[ ] Yes
[ ] No
[ ] Maybe
Comment: _____

32. If employees are connecting their personal devices to the business's network, does the business have policies regarding Bring Your Own Device ("BYOD") and Corporate Owned Personally Enabled ("COPE") devices in place?

[ ] Yes
[ ] No

[ ] Maybe
Comment: _____

If you would like further information or assistance from CyberCecurity, please visit our web site or contact us directly.