Cyber Supplemental Application

Applicant Information:

Name _____

Address _____
(street)

_____
(city, state, zip)

Industry _____

1. List ALL websites and email domains used by Applicant: _____
_____
_____

2. Annual revenue for the most recently completed fiscal year: _____

3. Total number of employees: _____

4. What is the estimated number of individuals for whom the Applicant stores or processes personal, health or credit card information?

   a. ◯ <100,000
   b. ◯ 100,001 – 250,000
   c. ◯ 250,001 – 500,000
   d. ◯ >500,000 (please provide an estimate _____)

5. Do you provide technology fraud/social engineering or security training (e.g. social engineering, phishing, spear phishing, baiting, etc.) for all of your employees? Yes ◯ No ◯

6. How often are systems and data on your computer network backed up? _____

7. Do you maintain offline backups that are:
   a. Automatically backed up? Yes ◯ No ◯
   b. Disconnected from your network OR stored with a cloud service provider? Yes ◯ No ◯
   c. Encrypted? Yes ◯ No ◯

8. Do you use multi-factor authentication (MFA) on:
   a. E-mail access? Yes ◯ No ◯
   b. Remote network access? Yes ◯ No ◯
   c. Privileged accounts (ie IT administrators' user accounts, access to cloud services)? Yes ◯ No ◯
   d. Backups? Yes ◯ No ◯

9. If MFA is <u>not</u> enabled on remote network access:
   a. Is RDP disabled on all computer network endpoints & servers? Yes ◯ No ◯
   b. Do you allow remote access to your computer networks? Yes ◯ No ◯

10. Do you use an email filtering tool (for example: Proofpoint, Barracuda, Mimecast)? Yes ◯ No ◯ If yes, what **specific brand** / **product** do you use? _____

11. Do you use an Endpoint Detection & Response Tool? Yes ◯ No ◯ If yes, what **specific brand** / **product** do you use? _____

12. Do you encrypt all sensitive information:
    a. At rest (ie on your networks / servers)? Yes ◯ No ◯
    b. On portable devices (laptops, mobile devices, portable backups)? Yes ◯ No ◯
    c. In transit / emailed? Yes ◯ No ◯

13. Do you have a process in place to download and install patches and critical updates onto your computer network (including all hardware and software publicly accessible through the internet):
    a. Within 5 days? Yes ◯ No ◯
    b. Within 30 days? Yes ◯ No ◯
    c. *If no to both, how often are patches & critical updates applied?* _____

14. Do you exclusively run supported operating systems on your computer network? Yes ◯ No ◯

15. Do you have procedures in place to verify authenticity of requests for payments or funds transfer, to confirm payment instructions are genuine / help detect and avoid social engineering scams? Yes ◯ No ◯

    If yes, describe procedures (for example dual authentication / callbacks to the requestor): _____

16. Do you have controls in place which require all fund and wire transfers over $25,000 to be verified and authorized by at least 2 employees prior to execution? Yes ◯ No ◯

17. Within the last 3 years, have you been subject to any complaints concerning the content of your website, advertising materials, social media or other publications? Yes ◯ No ◯

18. Do you enforce procedures to remove content (including 3rd party content) that may infringe or violate any intellectual property or privacy right? Yes ◯ No ◯

19. In the past 5 years, have you experienced any cyber attacks, system failures, data breaches, wire fraud incidents or other claims / incidents related to privacy and network security? Yes ◯ No ◯

    If yes, on a separate page, provide full details including dates, what exactly happened, how you secured systems, amounts paid, and changes made / new controls implemented to help avoid similar incidents in the future. If you had cyber insurance at the time, provide currently valued loss runs.

Signed: _____ Date: _____

Must Be Signed By an Executive Officer of the Parent Company

Name: _____

Please Print or Type