Pearl Cyber Questionnaire

Business Name _____

Company Website and/or email domain(s) _____

_____

Cyber Contact (First & Last) ** _____

Cyber Contact Email ** _____

** This contact person will receive cyber policy setup instructions, requests for payment, and policy documents

Is this business a law firm who derives more than 20% of revenue from real estate transactions? Yes☐ No☐

Business Type LLC ☐ Corporation ☐ Individual ☐ LP ☐ LLP ☐ Partnership ☐

Year Business Started _____ Projected Revenue _____

# of Employees (not IC's) _____ # of Independent Contractor's (Total) ___ IC Breakdown FT ___ PT ___

Desired Effective Date _____ **Desired Limit: 250k ☐ 500k ☐ 1mil ☐ Other _____**

Risk Management: (All questions must be answered. Please use the choices provided)

1. Has the organization ever suffered a cyber insurance claim? Yes☐ No☐ If YES – Date of last claim _____
2. Does the organization have knowledge or information regarding any fact, circumstance, situation, or event that could reasonably give rise to a claim or loss? Yes☐ No☐
3. Does the organization implement encryption on email sent to external parties, laptop computers, desktop computers, and other portable media devices? Yes☐ No☐
4. Does the organization collect, process, store, transmit, or have access to any Payment Card Information (PCI), Personally Identifiable Information (PII), or Protected Health Information (PHI) other than employees of the organization? Yes☐ No☐ If yes -
   - How many PII or PHI records does the customer collect, process, store, transmit, or have access to?
     Unknown☐ None☐ < 100k☐ 100-500k☐ 500k-1m☐ > 1mil☐
   - What is the estimated annual quantity of payment card transactions (credit cards, debit cards, etc.)?
     Unknown☐ None☐ < 100k☐ 100-500k☐ 500k-1m☐ > 1mil☐
5. Within the last 3 years has the organization been subject to any complaints concerning the content of its website, advertising materials, social media, or other publications? Yes☐ No☐
6. Does the organization enforce procedures to remove content (including third party content) that may infringe or violate any intellectual property or privacy right? Yes☐ No☐
7. Does the organization maintain at least weekly backups of all sensitive or otherwise critical data and all critical business systems offline or on a separate network? Yes☐ No☐
8. For which of the following services do you enforce Multi-Factor Authentication (MFA)?
   - Email: Yes☐ No☐ N/A – No Remote access allowed ☐
   - Virtual Private Network (VPN): Yes☐ No☐ N/A - No VPN allowed ☐
   - Remote Desktop Protocol (RDP), RD Web, RD Gateway, or other remote access:
     Yes☐ No☐ N/A – No remote access allowed ☐
   - Network / cloud administration or other privileged user accounts:
     Yes☐ No☐ On admin accts & cloud services where supported ☐
9. Does the organization require a secondary means of communication (a phone call) to validate the authenticity of
   - Any funds transfers (ACH, wire, etc.) Yes☐ No☐
   - Any requests to change banking details (ACH, wire, payroll etc) Yes☐ No☐
   - ➢ If No – Would the organization consider making these a requirement going forward? Yes☐ No☐
10. Does the organization have sensitive information stored on the cloud? Yes☐ No☐
11. Does the organization or its employees verify vendor/supplier bank information before adding to accounts payable systems? Yes☐ No☐ I don't have a formal accounts payable system ☐
12. Does the organization prevent unauthorized employees from initiating wire transfers? Yes☐ No☐
    - ➢ If No – Would the organization consider making this a requirement going forward? Yes☐ No☐