



**Accountants PROtectSM
Network Security And Privacy Liability
Supplemental Application**

BY COMPLETING THIS APPLICATION, THE APPLICANT IS APPLYING FOR COVERAGE WITH EITHER **COLONY INSURANCE COMPANY**, **COLONY SPECIALTY INSURANCE COMPANY** OR **PELEUS INSURANCE COMPANY**, AN AUTHORIZED SURPLUS LINES INSURER OR **ARGONAUT INSURANCE COMPANY**, A LICENSED INSURER.

INSTRUCTIONS –

- Answer all questions. The information provided herein is considered material to our underwriting and pricing decision for the policy or additional coverage under consideration at the time this supplemental application is submitted.
- For any information that exceeds the space provided, continue responses on your letterhead.
- This form must be completed, dated and signed by an authorized officer of the Applicant to include this completed form as part of the Application.

1. Name of Applicant:

2. a. Does the Firm provide remote access to its computer systems? Yes No
b. How many users have remote access?
c. Is remote access restricted to Virtual Private Networks (VPNs)? Yes No

3. a. Does the Firm have documented procedures in place for user and password management? Yes No
b. Describe password requirements:

4. a. Does the Firm use a firewall to prevent unauthorized access? Yes No
b. If "Yes", please provide full details.

5. a. Does the Firm terminate all associated computer access and user accounts as part of the regular exit process when an employee leaves the company? Yes No
b. Does the Firm regularly compare all computer access/user accounts with a comprehensive employee record to identify potential unauthorized users/accounts? Yes No

6. a. Does the Firm have a formal procedure for the disposal of obsolete computers or hard drives? Yes No
b. If "Yes", please provide full details.

7. a. Does the Firm currently have a website? Yes No
- b. If "Yes", please check all that apply:
- | |
|---|
| <input type="checkbox"/> Content from others, including attachments and links to other websites |
| <input type="checkbox"/> Secure consent and any necessary licensing and/or releases |
| <input type="checkbox"/> Use of disclaimers pertaining to content made available |
| <input type="checkbox"/> User account access and interactivity |
| <input type="checkbox"/> User can download information |
| <input type="checkbox"/> User can upload information |
| <input type="checkbox"/> Other (describe): |
8. a. Does the Firm accept payment on-line for goods sold or services rendered? Yes No
- b. If "Yes", is the Firm PCI compliant? Yes No
9. a. Does the Firm have a virus protection program in place? Yes No
- b. If "Yes", please provide full details.
-
- c. Does the Firm regularly implement patches on its network? Yes No
- d. If "Yes", how often?
10. a. Does the Firm back up data daily? Yes No
- b. If "Yes", are data backups stored off site? Yes No
- Does the Firm have a formal policy regarding the security of client files removed from the office? Yes No
11. Does the Firm have a written disaster recovery and business continuity plan for network systems? Yes No
12. a. Does the Firm have an incident response plan in place? Yes No
- b. How long would it take to restore operations after a computer attack?
13. Does the Firm have physical security controls in place to control access to network systems? Yes No
14. Does the Firm conduct training for every employee user of the network systems in security issues and procedures? Yes No
15. a. Does the Firm employ intrusion detection/intrusion protection devices on their network? Yes No
- b. How often are intrusion logs reviewed?
16. a. Does the Firm have a program in place to periodically test security controls? Yes No
- b. Does the Firm conduct information security/privacy compliance evaluations? Yes No
- c. For both parts, if "Yes", is such testing done by an outside third party? Yes No
17. Have you ensured that all sensitive business/consumer information that resides within your organization's systems has been encrypted while 'at rest' within databases or other electronic data files? Yes No
18. Have you ensured that all sensitive business/consumer information that is physically transmitted via tape or any other medium between your organization's facilities and those of your business partners/service providers has been encrypted? Yes No

19. a. Inception Date of the Firm's first Cyber Policy:
- b. Desired Retroactive Date:
20. a. Does the Firm outsource any aspect of the computer network or security processes (hosting, back up, firewall, etc.)? Yes No
- b. If "Yes", please provide full details.
21. a. Does the Firm require all vendors, to whom they outsource data or hosting functions, to demonstrate adequate security of their computer systems? Yes No
- b. If "Yes", please indicate method of verification:
- | | |
|---|--|
| <input type="checkbox"/> Vendor must supply SAS 70 or CICA Section 5970 | |
| <input type="checkbox"/> Security is assessed by internal staff, if selected, is this done at least annually? | <input type="checkbox"/> Yes <input type="checkbox"/> No |
| <input type="checkbox"/> Other, describe: | |
22. Does the Firm have procedures to ensure compliance with legal regulatory and/or contractual privacy requirements? Yes No

THIS SUPPLEMENTAL APPLICATION IS INCORPORATED BY REFERENCE INTO THE PRIMARY APPLICATION

APPLICANT'S SIGNATURE	DATE
-----------------------	------