



**Cyber Tech PROtectSM
New Business Application**

IMPORTANT NOTICE

THIS IS AN APPLICATION FOR A POLICY THAT IS WRITTEN ON A CLAIMS-MADE BASIS AND COVERS ONLY CLAIMS FIRST MADE AGAINST THE INSUREDS DURING THE POLICY PERIOD OR THE EXTENDED REPORTING PERIOD, IF EXERCISED. CLAIMS MUST BE REPORTED TO THE INSURER IN ACCORDANCE WITH THE REPORTING PROVISIONS OF THE POLICY. THE LIMITS OF LIABILITY SHALL BE REDUCED, AND MAY BE COMPLETELY EXHAUSTED BY AMOUNTS INCURRED AS DEFENSE COSTS. PLEASE READ THE POLICY CAREFULLY AND DISCUSS THE COVERAGE PROVIDED WITH YOUR INSURANCE AGENT OR BROKER.

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.

GENERAL INFORMATION

1. Name of Applicant _____
2. Address of Applicant _____
3. Business Phone _____
4. State of Incorporation _____
5. Date Established _____
6. Web Address of Applicant _____
7. Risk Management Contact Information – Name and Email Address _____

8. Company Type: Sole Proprietor Corporation Partnership Professional Corporation Franchise
 LLC Non-Profit Other (describe) _____

9. Revenue:

	Past Year	% of Online Revenue	Current Year	% of Online Revenue	Next Year	% of Online Revenue
United States	\$	%	\$	%	\$	%
Other than the United States	\$	%	\$	%	\$	%

10. # of employees:

	Current Year
United States	
Other than the United States	

11. Business Description

- a. Will there be any significant changes to the nature or size of the Applicant’s business in the next twelve (12) months or have there been any such changes in the past twelve (12) months? Yes No
 If “Yes”, explain.

12. Current Coverage

Coverage	Carrier	Policy Period	Limit	Deductible	Premium
Cyber		From:	\$	\$	\$
		To:			
MPL		From:	\$	\$	\$
		To:			
Tech E&O		From:	\$	\$	\$
		To:			
Media		From:	\$	\$	\$
		To:			

SECTIONS A and B – PRIVACY AND SECURITY COVERAGE

1. Does the Applicant have a chief privacy officer? Yes No
 If “No”, what functionally equivalent position is responsible for management of, and compliance with the applicant’s privacy policies? _____
2. Does the Applicant have a written corporate-wide privacy policy? Yes No
 If “Yes”, what position is responsible for creating, updating and managing compliance with such privacy policy?

3. Does the Applicant post a privacy policy on its internet website? Yes No
 If “Yes”,
 a. Has the policy been reviewed by a qualified attorney? Yes No
 b. When was it last updated? _____
4. Does the Applicant have an asset classification program that includes a data classification standard (e.g., public, internal use only, confidential)? Yes No
 If “Yes”, does this program also include mandated requirements for heightened protections (e.g., encryption, access control, data handling, retention and eventual destruction) that accompany each classification level? Please describe.

5. What sensitive information does the Applicant collect, store, maintain, process, transmit or otherwise control? (Check all that apply and provide approximate number of records.)

- Social Security Numbers _____
- Credit/Debit Card Numbers _____
- Drivers License Numbers _____
- Government ID Numbers _____
- Financial Account Numbers _____
- Medical Records/Protected Health Information _____
- Credit History and Ratings _____
- Intellectual Property of Others _____
- Other (describe) _____

6. What was the Applicant's approximate percentage of revenues from credit card and debit card transactions in the most recent twelve (12) months? _____

Approximately how many credit card and debit card transactions are processed annually? _____

- a. Card Present _____
- b. Card not present/on-line purchases _____

7. If the Applicant accepts credit cards for payment of goods and services, is the Applicant compliant with applicable data security standards issued by financial institutions the Applicant transacts business with (e.g., PCI standards)? If "No", explain. Yes No

8. Is the Applicant compliant with applicable data security standards issued by the following (check all that apply):

- Sarbanes-Oxley EU-US Safe Harbor Framework Agreement Gramm-Leach Bliley Act 1999
- HIPAA/HITECH Identity Theft Prevention Program (i.e., FTC Red Flags)
- Do Not Track Laws (if applicable) European Union Data Protection Directive (GDPR)
- Other (describe): _____

9. Prior to hiring personnel, does the Applicant conduct background checks with respect to employment history, drug, criminal record, credit history and reference checks? Yes No
If "Yes", is this completed for all employees or just some?
Is it completed for independent contractors? Yes No

10. Does the Applicant provide employees with formal training with respect to personally identifiable information on at least an annual basis? Yes No

11. Does the Applicant require third parties with which it shares personally identifiable information or confidential information to indemnify Applicant for legal liability arising out of the release of such information due to the fault or negligence of the third party? Yes No

12. Does the Applicant restrict employee access to personally identifiable information on a business-need to know basis? Yes No

13. Has the Applicant configured their organization's internet-facing web sites and related systems so that no sensitive customer data resides directly on these systems? Yes No

14. Has the Applicant configured their network to ensure that access to sensitive customer's data is limited to properly authorized requests to internal databases/systems that are otherwise fully protected against internet access? Yes No

15. Does the Applicant sell or share individual subscriber or user identifiable information with other internal or external entities? If "Yes", explain. Yes No

16. Is the Applicant aware of any release, loss or disclosure of personally identifiable information in its care, custody or control, or anyone holding such information on behalf of the Applicant in the most recent three year time period from the date of this application? Yes No

17. Does the Applicant have written policies in place which address:
a. Network security? Yes No
b. Appropriate use of network resources on the internet? Yes No
c. Appropriate use of email? Yes No

18. Has a network security assessment or audit been conducted within the past twenty-four (24) months? Yes No
If "No", when was the last audit completed? _____
Were any deficiencies identified? Yes No
If "Yes", have corrective measures been addressed/implemented? Yes No

19. Does the Applicant conduct periodic intrusion detection, penetration or vulnerability testing? Yes No
If "Yes", please describe what is done, the frequency, and who performs the work?

20. Are patches implemented on network appliances (routers, bridges, firewalls, etc.) to mitigate current vulnerabilities? If "Yes", how often are patches installed? Yes No _____

21. Are Applicant's systems backed up on a daily (or more regular) basis? Yes No
If "No", how often are systems backed up? _____
Are data backups stored offsite? Yes No

22. Are data recovery and restoration procedures tested? Yes No
If "Yes", how frequently? _____

23. Does the Applicant have a written disaster recovery and business continuity plan for its network? Yes No
Is the plan tested? Yes No
If "Yes", describe frequency and extent of testing.

What are the recovery time objectives for critical applications?

24. Does the Applicant actively maintain system logs on all mission-critical servers and appliances? Yes No
Are logs regularly checked for irregularities, intrusions or violations? Yes No
If "Yes", how often are logs checked and who holds this responsibility? _____

25. Are documented procedures in place for user and password management? Yes No
If "Yes", are they monitored for compliance? Yes No
Are users required to use unique/strong passwords of at least six (6) characters? Yes No

26. Are the Applicant's dedicated computer rooms physically protected? Yes No
If "Yes", describe and include how access is controlled or limited (e.g., key cards, biometrics, etc.)?

27. Does the Applicant have a formal Incident Response Plan for determining the severity of a potential data security breach and providing prompt notification to all individuals who may be adversely affected by such exposures? Yes No
 Has the plan been tested? Yes No
 If "Yes", what was the date of the most recent tabletop exercise? _____

28. Does the Applicant have and use the following technological defenses:

- a.** Firewalls? Yes No
 If "Yes", is it used at all internet points-of-presence to prevent unauthorized access to internal networks? Yes No
- b.** Anti-virus? Yes No
 If "Yes",
 - i.** Are antivirus applications updated in accordance with the software providers requirements? Yes No
 - ii.** Is the anti-virus software used on all desktops, portable devices and mission critical servers? Yes No
- c.** Intrusion detection? Yes No
- d.** Data loss prevention? Yes No

If "No", describe the alternative controls implemented to prevent unauthorized access or intrusion to computer systems?

29. Does the Applicant ensure that all sensitive business and consumer information that is transmitted has been encrypted using industry-grade mechanisms? Yes No

30. Does the Applicant ensure that all sensitive business and consumer information that resides within their systems has been encrypted while "at-rest"? Yes No

31. For computer equipment that leaves Applicant's physical facilities (e.g., mobile laptops, PDAs, Blackberry's and home-based desktops), has Applicant implemented strong access control requirements and/or hard drive encryption to prevent unauthorized exposure of company data in the event these devices are stolen, lost or otherwise unaccounted for? Yes No

32. Does the Applicant follow established procedures for carrying out and confirming the destruction of:

- a.** Data residing on systems or devices prior to their recycling, refurbishing, resale, or physical disposal? Yes No
- b.** Sensitive information in electronic and paper form prior to recycling or physical disposal? Yes No

33. Does the Applicant terminate all computer access and user accounts as part of the regular exit process when an employee leaves the company or when a third party contractor no longer provides the contracted services? Yes No

SECTIONS C and D – MPL AND TECHNOLOGY PRODUCTS & SERVICES LIABILITY COVERAGE

1. Provide information on the Applicants three (3) largest clients:

Client Name	Client Industry	Services Performed	% of Revenue
			%
			%
			%

- 2. Does the Applicant use independent contractors and/or subcontractors? Yes No
- 3. Does the Applicant require independent contractors to carry professional liability insurance? Yes No
- 4. Do contracts with independent contractors and subcontractors contain:
 - a. Indemnification/hold harmless for their work product? Yes No
 - b. Ownership of intellectual property rights? Yes No

- 5. In the last five (5) years:
 - a. Has the Applicant provided professional services to clients in which the Applicant or any related individual served as an officer, director, trustee, or partner? If "Yes", explain. Yes No

- b. Has the Applicant provided professional services to clients in which the Applicant or any related individual owned an equity or financial interest? If "Yes", explain. Yes No

- 6. What % of the Applicant's revenues for products or services are purchased or provided under the following types of agreements:

Applicant's Standard Contract Wording	Client Contract Wording	No Written Agreement
%	%	%

Provide a specimen copy of Applicant's contract with clients.

- 7. Identify which of the following provisions are included in Applicant's standard contract wording with Applicant's clients:

Provision	In Favor of Applicant	In Favor of Client	Mutually Beneficial	N/A
Hold Harmless	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Indemnification	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Limitation of Liability	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Ownership of Intellectual Property	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Disclaimer of Warranties	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

- 8. How does Applicant manage the review and approval of client contract wording or modifications to Applicant's contract wording?

- 9. How many times have Applicant sued a client for fees in the last three (3) years? _____

- 10. If the Applicant provides software, hardware or information services, which of the following risk management practices does the Applicant employ (check all that apply):

- Secure coding practices
- Developer testing
- Escalation process for client complaints
- User acceptance testing
- Client sign-off on specifications
- Client sign-off at project milestones
- Client sign-off on final delivery
- Beta testing
- N/A

- 11. Does the Applicant have membership(s) in any professional organizations, associations or societies? Yes No
If "Yes", please list the name of the organization, association or society. _____

- 12. Has the Applicant provided professional liability services within the past five (5) years to clients who subsequently entered into bankruptcy or receivership? Yes No

13. Does the Applicant have a written quality control document and/or a formal procedure for screening and evaluating new clients? If "Yes", explain. Yes No

14. Do all professional employees comply with applicable continuing education requirements? Yes No

15. Does the Applicant have a social engineering fraud risk management strategy in place, including an employee training and awareness program? Yes No

16. Does the Applicant independently verify written, electronic or telephonic instructions to transfer, pay or deliver funds or data with call-backs to senior management at a previously known or designated phone number? Yes No

17. In the last five (5) years, have any of the following events involving a professional service ever been made against the Applicant?

- a. Claims? Yes No
- b. Potential claims? Yes No
- c. Subject of a complaint to authorities or disciplinary action? Yes No
- d. Received any complaints concerning products or services provided by the Applicant or anyone else on behalf of the Applicant? Yes No

If "Yes", please provide details and note if reported to an insurance policy.

SECTION E – MEDIA LIABILITY COVERAGE

1. Please indicate the content posted on the Applicant's website (check all that apply):
- No website Unlicensed third party content (e.g., blog, message boards, customer reviews)
 - Content under license from a third party Information created by the Applicant
 - Streaming video or music content

2. Does the Applicant have a procedure for responding to allegations that content in any form created, displayed, or published by the Applicant is libelous, infringing, or in violation of a third party's privacy rights? Yes No

3. Does the Applicant have a process to review content in any form prior to publication through any medium including but not limited to posting it on the Applicant's website? Yes No

If "Yes",

- a. Is the review performed by a qualified attorney? Yes No
- b. Does the review include screening the content for the following:
 - i. Disparagement issues? Yes No
 - ii. Copyright infringement? Yes No
 - iii. Trademark infringement? Yes No
 - iv. Invasion of privacy? Yes No

If there is no process, please explain what the Applicant does to avoid the posting of improper or infringing content.

4. Has the Applicant acquired any trademarks from others in the past five (5) years and if so, were the trademarks screened for infringement? Yes No
5. Does the Applicant disseminate any content which includes material supplied by customers, contractors or vendors? If "Yes", check all that apply: Yes No
- Require the third party to hold Applicant harmless for any defamatory or infringing content supplied to Applicant
 - Obtain all necessary licenses for this content
 - Have a process in place to monitor compliance licenses for third party content (including open source software licenses)
6. Does the Applicant post third party content on their website? Yes No
- If "Yes", does the Applicant have policies in place (take down protocols, etc.) to comply with the safe harbor provisions of the Digital Millennium Copyright Act and the Communications Decency Act? Yes No
7. Does the Applicant require employees and contractors to affirm in writing that they will not use content created for prior employers or customers? Yes No
8. Does the Applicant have a social media policy for employees and contractors acting on Applicant's behalf that addresses:
- a. Maintaining customer/patient confidentiality? Yes No
 - b. Personal posts related to Applicant's business? Yes No
 - c. Infringement of third party intellectual property rights? Yes No
 - d. Defamation of competitors and others? Yes No
 - e. Comments / claims regarding Applicant's business, products or services? Yes No
9. Within the last five (5) years, has the Applicant ever received a complaint or cease and desist demand alleging trademark, copyright, invasion of privacy, or defamation with regard to any content published, displayed or distributed by or on behalf of the Applicant? Yes No
- If "Yes", please provide details and note if reported to an insurance policy.
-
10. Has the Applicant's legal counsel checked that Applicant's domain name(s) and metatags do not infringe on another's trademark? Yes No

WARRANTY STATEMENTS

- Does the Applicant, predecessors in business or any other person for whom coverage is requested, have knowledge of any actual or alleged act, error, omission or circumstance which may result in a claim being made against them or any other basis to reasonably anticipate a claim being made against them? Yes No
- If "Yes", has the Applicant reported same to the Applicant's current insurer? Yes No
- If "Yes", please complete a Claims Supplemental Application or attach a statement providing full details.

FRAUD STATEMENT/SIGNATURES

THE FRAUD STATEMENT APPLICABLE TO YOU APPEARS ON THE FOLLOWING PAGE OF THIS INSURANCE APPLICATION. PLEASE READ IT CAREFULLY AND SIGN YOUR APPLICATION.

FRAUD STATEMENT**(Not applicable in the states mentioned below where a specific warning applies.)**

Any person who knowingly and with intent to defraud any insurance company or other person files an application for insurance or statement of claim containing any materially false information, or conceals for the purpose of misleading, information concerning any fact material thereto, may be committing a fraudulent insurance act, and may be subject to a civil penalty or fine.

Alabama

Any person who knowingly presents a false or fraudulent claim for payment of a loss or benefit or who knowingly presents false information in an application for insurance is guilty of a crime and may be subject to restitution, fines, or confinement in prison, or any combination thereof.

Arkansas, District of Columbia, Louisiana, Rhode Island, West Virginia

Any person who knowingly presents a false or fraudulent claim for payment of a loss or benefit or knowingly presents false information in an application for insurance is guilty of a crime and may be subject to fines and confinement in prison.

Colorado

It is unlawful to knowingly provide false, incomplete, or misleading facts or information to an insurance company for the purpose of defrauding or attempting to defraud the company. Penalties may include imprisonment, fines, denial of insurance and civil damages. Any insurance company or agent of an insurance company who knowingly provides false, incomplete, or misleading facts or information to a policyholder or claimant for the purpose of defrauding or attempting to defraud the policyholder or claimant with regard to a settlement or award payable for insurance proceeds shall be reported to the Colorado Division of Insurance within the Department of Regulatory Agencies.

Florida

Any person who knowingly and with intent to injure, defraud, or deceive any insurer files a statement of claim or an application containing any false, incomplete, or misleading information is guilty of a felony of the third degree.

Kansas

Any person who, knowingly and with intent to defraud, presents, causes to be presented or prepares with knowledge or belief that it will be presented to or by an insurer, purported insurer, broker or any agent thereof, any written statement as part of, or in support of, an application for the issuance of, or the rating of an insurance policy for personal or commercial insurance, or a claim for payment or other benefit pursuant to an insurance policy for commercial or personal insurance which such person knows to contain materially false information concerning any fact material thereto; or conceals, for the purpose of misleading, information concerning any fact material thereto commits a fraudulent insurance act.

Kentucky

Any person who knowingly and with intent to defraud any insurance company or other person files an application for insurance containing any materially false information or conceals, for the purpose of misleading, information concerning any fact material thereto commits a fraudulent insurance act, which is a crime.

Maine

It is a crime to knowingly provide false, incomplete or misleading information to an insurance company for the purpose of defrauding the company. Penalties may include imprisonment, fines or denial of insurance benefits.

Maryland

Any person who knowingly or willfully presents a false or fraudulent claim for payment of a loss or benefit or who knowingly or willfully presents false information in an application for insurance is guilty of a crime and may be subject to fines and confinement in prison.

New Jersey, New Mexico

Any person who knowingly presents a false or fraudulent claim for payment of a loss or benefit or knowingly presents false information in an application for insurance is guilty of a crime and may be subject to civil fines and criminal penalties.

Ohio

Any person who, with intent to defraud or knowing that he is facilitating a fraud against an insurer, submits an application or files a claim containing a false or deceptive statement is guilty of insurance fraud.

Oklahoma

WARNING: Any person who knowingly, and with intent to injure, defraud or deceive any insurer, makes any claim for the proceeds of an insurance policy containing any false, incomplete or misleading information is guilty of a felony.

Oregon

Any person who knowingly and with intent to defraud or solicit another to defraud the insurer by submitting an application containing a false statement as to any material fact may be violating state law.

Pennsylvania

Any person who knowingly and with intent to defraud any insurance company or other person files an application for insurance or statement of claim containing any materially false information or conceals for the purpose of misleading, information concerning any fact material thereto commits a fraudulent insurance act, which is a crime and subjects such person to criminal and civil penalties.

Pennsylvania (Auto)

Any person who knowingly and with intent to injure or defraud any insurer files an application or claim containing any false, incomplete or misleading information shall, upon conviction, be subject to imprisonment for up to seven years and the payment of a fine of up to \$15,000.

Tennessee, Virginia, Washington

It is a crime to knowingly provide false, incomplete or misleading information to an insurance company for the purpose of defrauding the company. Penalties include imprisonment, fines and denial of insurance benefits.

New York

Any person who knowingly and with intent to defraud any insurance company or other person files an application for insurance or statement of claim containing any materially false information, or conceals for the purpose of misleading, information concerning any fact material thereto, commits a fraudulent insurance act, which is a crime, and shall also be subject to a civil penalty not to exceed five thousand dollars and the stated value of the claim for each such violation.

New York (Auto)

Any person who knowingly makes or knowingly assists, abets, solicits or conspires with another to make a false report of the theft, destruction, damage or conversion of any motor vehicle to a law enforcement agency, the department of motor vehicles or an insurance company, commits a fraudulent insurance act, which is a crime, and shall also be subject to a civil penalty not to exceed five thousand dollars and the value of the subject motor vehicle or stated claim for each violation.

SIGNATURES

DO NOT SIGN UNTIL YOU HAVE READ THE CONTENTS OF THIS APPLICATION AND THE APPLICABLE FRAUD WARNING(S).

I have reviewed the contents of this application and with my signature, I declare to the best of my knowledge that all statements herein are true and no material facts have been suppressed or misstated. I am also aware that my operation may be inspected by the Insurance Company.

APPLICANT/NAMED INSURED	
APPLICANT/NAMED INSURED SIGNATURE	DATE

Agent/Broker:

Are you personally familiar with this Applicant's operations?

Yes No

Did your office control this risk in the past year?

Yes No

AGENT'S OR BROKER'S NAME AND ADDRESS	TELEPHONE NUMBER	LICENSE NO.
AGENT'S OR BROKER'S SIGNATURE		DATE