Admiral INSURANCE GROUP | a Berkley Company

AdmiralPro Delta® TEC

PROFESSIONAL LIABILITY APPLICATION
(CLAIMS MADE AND REPORTED COVERAGE)

NOTICE TO APPLICANT: By signing this application you agree the answers you give us in this application and any other information you give us as part of the application process are:

1. **Accurate & Complete.**
2. **Given to us to issue you an insurance policy.**
3. **Material to our decision-making process in issuing you an insurance policy.**
4. **A significant part of what we relied upon in making our decision in issuing you an insurance policy. You must agree to notify us, through your insurance brokerage, if during the policy term any material changes to your operations occur.**

SECTION I – INTRODUCTION

1) Legal Name of Applicant:

2) Please list all subsidiaries:

3) Applicant's address:

4) FEIN:

5) Where can we find you on the internet? (Please list all URLs registered in your name)

6) Is this your first time purchasing this coverage? ◯ Yes ◯ No
If No, provide the following information about your most recent policy so we can better understand how we can help:

Limits of Liability	$ / $
Expiration Date	
SIR/Deductible	$
Retro Date(s)	
Insurance Company	
Premium	$

7) How many people work for you? List the number of each.

Principals, Partners Officers	
Technical Personnel	
Independent Contractors	
Clerical & Support	
Sales & Marketing	
Other:	
TOTAL	

SECTION II – GETTING TO KNOW YOU

1) How long have you been in business?

2) Describe your business operations:

3) Describe an ideal end use of your product or service:

4) Did your business have any prior names? ◯ Yes ◯ No
If Yes, provide complete details:

5) Have you experienced any mergers, acquisitions or divestitures in the last 5 years? ◯ Yes ◯ No
Do you plan on any within the next 12 months? ◯ Yes ◯ No
If Yes, provide complete details:

6) Are you controlled by any other entity? ◯ Yes ◯ No
If Yes, provide complete details:

7) Do you offer any products or services that are not technology related? ◯ Yes ◯ No
If Yes, provide complete details:

8) In the last fiscal year, what percentages of your revenue were from the following activities?

(This section should total 100%)

Activities	Percentage	Activities	Percentage
Application Service Provider	%	Managed Service Provider	%
Automation & control Systems Software Development, Integration, Sales & Support (No Engineering)	%	Medical Billing and Other Billing Services – Services for a Third Party for a Fee	%
Call Center Services	%	Mobile Application Software Development – Not Proprietary	%
Cloud Computer, Co-Locating Services, Electronic Data Storage	%	Monitoring (Real Time) Software Development & Sales – No Monitoring or Alert Services	%
Computer Hardware Maintenance, Assembly, Repair – Not Proprietary	%	Monitoring (Real Time) Software Development & Sales Including Monitoring or Alert Services	%
Computer Skills Training & Education	%	Network Security Consulting & Security Audits (no real time monitoring)	%
Contract Programming Services & Temporary Staffing (NOC) – Insured Employs Staff Being Placed	%	Payment Processors / Gateway	%
Custom Software Development & Licensing (NOC)	%	Privacy Law based Regulatory Compliance Consulting	%
Data Aggregation Services (not in the Insured's own data)	%	SaaS – Software as a Service Provider	%
Data Destruction Services (Electronic or Physical Data)	%	Technology Consulting – Not Proprietary	%
Disease Management Platform	%	Technology Product Design & Development for Others – Not Insured's Proprietary Product	%
GIS / GPS / Mapping / Modeling Software	%	Technology Staffing (Permanent) & Recruiting (insured is not employer or staff being placed)	%
Graphic Design & Branding Services	%	Telecommunications System Design, Integration, Consulting	%
Hardware & Software Installation & Integration – Not Proprietary	%	Telemedicine Platform & Referral Services	%
Health Information Exchange	%	Value-Added Reseller of Non-Proprietary Hardware and Software	%
Health Information Portal for Consumer Healthcare Inquiries	%	Website Design & Development for Others	%
Internet Service Provider	%	Other:	%

9) In the last fiscal year, provide the percentage of revenue attributed to the following types of clients.
(This section should total 100%)

Type of Clients	Percentage
Aerospace	%
Architects / Engineers	%
Automotive	%
Casino / Gaming	%
Construction Industry	%
Educational Institutions	%
Energy & Power Generation	%
Entertainment / Athletics	%
Federal Government	%
Financial Institutions	%
Healthcare	%

Hospitality	%
Individual Consumers	%
Law Enforcement	%
Local Government	%
Manufacturing	%
Oil & Gas	%
Recreational	%
Retail	%
Transportation	%
Utilities	%
Other:	%
TOTAL:	100%

10) REVENUES: (Revenue can be sales, capital funding, grants, etc.)

	Actual Prior Year	Current FY Projection	Next Year Projection
U.S. Revenue	$	$	$
Foreign Revenue	$	$	$
Total Revenue	$	$	$
Capital Funding	$	$	$

11) Do you have employees in countries other than the USA? ◯ Yes ◯ No
If Yes, provide complete details:

12) Do you have foreign office locations and/or foreign employees? ◯ Yes ◯ No
If Yes, provide details including list of countries, number of employees and revenue associated with each:

13) Five largest projects in the last three years?

Client	Services Rendered	Project Duration	Revenue Derived

14) Do you subcontract any of your services to others? ◯ Yes ◯ No
If Yes, describe these operations

15) Do you require subcontractors, independent contractors or third-party vendors to carry insurance? ◯ Yes ◯ No
If Yes, does that requirement include coverage for:

Coverage	Yes / No	Minimum Limits of Liability
Network Security and Data Privacy	◯ Yes ◯ No	
General Liability	◯ Yes ◯ No	
Professional Liability	◯ Yes ◯ No	

SECTION III – YOUR RISK

1) Describe the most likely result if your product or service failed to perform as intended:

2) Is there an acceptable downtime for your customers if your product or service fails? ◯ Yes ◯ No
If Yes:

- ☐ Less than 1 day
- ☐ Less than 2 days
- ☐ More than 2 days

3) Do you use written contracts or agreements with your clients on 100% of your products and services? ◯ Yes ◯ No

If No, what percentage of your clients sign contracts? ____ %

4) Do your clients provide written acceptance and approval of the work you complete? ◯ Yes ◯ No

5) What percentage of your revenue comes from the sale of a product or software developed by another company? ____ %

6) Is all software development work for others documented and tested before deployment? ◯ Yes ◯ No

7) Have you discontinued any software, product, or service in the last five years? ◯ Yes ◯ No

If Yes, have you continued to provide maintenance services after discontinuance? ◯ Yes ◯ No
Describe:

SECTION IV – NETWORK SECURITY & DATA PRIVACY

*For each and every claim, click the link to complete the Supplemental Claim Information Form.

1) a. Where do your servers reside?

☐ Cloud ☐ On Premises

b. If cloud, which vendor(s) do you use?

c. Are your production servers separated in different locations? ◯ Yes ◯ No

2) Is your network managed in house or by a vendor? ◯ Yes ◯ No

If outsourced, which vendor(s) do you use?

What are the qualifications of your IT security leaders? (Examples: CISSP, CISM, CISA, CEH, CCSP)

3) Indicate all IT risk management elements implemented by your vendor:

	In-House	Vendor		In-House	Vendor
Access Restrictions			Hot Site		
Anti-Virus Scanning			Load Balancers		
Automated Security Scanning			Proxy Servers		
Network Intrusion Detection			Security Audits		
Encryption			Secure Remote Capabilities		
Firewall			Others:		

4) How frequently do you test your network security to ensure effectiveness and response time?

☐ Monthly ☐ Quarterly ☐ Annually

5) What are your procedures for correcting vulnerabilities from penetration testing?

6) Do you host or access sensitive information (medical records, financial records, protected personal information)? ◯ Yes ◯ No

If Yes, how many records do you access?

7) Are the following encrypted?

☐ Sensitive and/or Confidential Information

☐ Remote Access

☐ All Information

☐ Data in Transit

8) Do you have a privacy policy? ◯ Yes ◯ No

If Yes, has it been reviewed by legal representation? ◯ Yes ◯ No

9) Do you require security training for employees and contractors which includes strategies to recognize email-based ransomware and phishing attacks? ◯ Yes ◯ No

10) a. How often do you purge data?

b. Check the following safeguards that you use for data destruction:

- ☐ Physical Destruction – Certification from vendor for physical shredding of media.
- ☐ Overwriting – Single or multiple overwriting passes with fixed pattern such as binary zeroes.
- ☐ Degaussing – Strong magnetic field applied to magnetic media to randomize field orientation.

11) How do you ensure sensitive data destruction compliance with applicable privacy law?

12) Do you use any physical security controls to prevent unauthorized access to networks and data? (Examples: controlled swipe card access with logging, security cameras, etc.) ◯ Yes ◯ No
If Yes, describe such controls:

13) a. How often are networks backups performed?

b. How often are these backups tested?

c. Are the backups stored offsite? ◯ Yes ◯ No

14) a. How often is your disaster recovery plan tested?

b. What is your recovery time objective? *(This is the time it takes to recover from an event.)*

c. What is your recovery point objective? *(This is the point in time to which you are restoring or how far back in time prior to an event that the last known backup or last known good configuration is known to exist.)*

15) a. How often do you patch:

Server infrastructure:

Desktop/laptop infrastructure:

b. If you are a software company, how often do you issue patches?

c. Are you responsible for patching any systems for customers? ◯ Yes ◯ No

If Yes, how frequently?

d. How do you respond to Zero-Day vulnerabilities? *(A Zero-Day vulnerability or exploit is a vulnerability that has been disclosed but not yet patched. Recent example: log4j.)*

16) What types of network monitoring solutions, active and passive, do you have in place and who does the monitoring?

17) What are your data security vetting procedures for third parties that you either share data or network access to?

18) a. Are you subject to:

	Date of Last Audit/Assessment
Health Information Portability and Accountability Act (HIPAA)	
Biometric Information Privacy Act (BIPA)	
Health Information Technology for Economic and Clinical Health Act (HITECH)	
Payment Card Industry Data Security Standards (PCI DSS)	
SOC II Certification Type I	
SOC II Certification Type II	

b. If you are subject to PCI DSS, what is your certification level?

SECTION V – RANSOMWARE

SECTION A – SECURITY CONTROLS

1) Do you employ:

a. Endpoint Detection and Response (EDR) security tools? ◯ Yes ◯ No

b. Multi-Factor Authentication for the following:

Critical Information ◯ Yes ◯ No

Remote Access ◯ Yes ◯ No

Administrator and privileged user accounts ◯ Yes ◯ No

Personal devices accessing the network ◯ Yes ◯ No

Independent contractors and vendors accessing the network ◯ Yes ◯ No

Non-critical information and applications ◯ Yes ◯ No

c. Are workstations prohibited from local admin rights? ◯ Yes ◯ No

All the time or case by case?

Do you manage privileged accounts using tooling such as CyberArk or other? ◯ Yes ◯ No

How many users have persistent privileged accounts for endpoints (defined as those who have entitlements to configure, manage, and support endpoints)?

Please describe compensating security controls for these specific persistent privileged accounts:

d. Network segmentation to separate critical systems, applications and data from non-critical? ◯ Yes ◯ No

2) Do you route all outbound web requests through a web proxy which monitors for and blocks potentially malicious content? ◯ Yes ◯ No

3) Are external emails tagged as such to alert your employees that the email originated from outside of your organization? ◯ Yes ◯ No

4) Do you utilize Microsoft Office 365? ◯ Yes ◯ No

If Yes, does this include Office 365 Threat Protection add-on? ◯ Yes ◯ No

If you answered No to any of the above questions, or you use an alternative product to MS Office 365, provide an explanation as to why this measure has not been implemented:

SECTION B – INTERNAL TRAINING AND PROCEDURES

5) Do you conduct at least yearly employee training related to:

a. Company Incident Reporting Procedures ◯ Yes ◯ No

b. Document Management ◯ Yes ◯ No

c. Internet and Email Use ◯ Yes ◯ No

d. Passwords ◯ Yes ◯ No

e. Responsibility for Company Data ◯ Yes ◯ No

6) Do you conduct at least annual employee cyber competence testing such as:

a. Social engineering attacks (i.e. Phishing, baiting, scareware, etc.) ◯ Yes ◯ No

b. Physical security (locked and secured computer devices) ◯ Yes ◯ No

7) Do you require encryption of PII/PHI files while:

a. In transit ◯ Yes ◯ No

b. At rest ◯ Yes ◯ No

c. How are your encryption keys protected?

8) Do you have rapid (immediate) account access termination procedures for employees that leave the company? ◯ Yes ◯ No

If you answered No to any of the above questions, provide an explanation as to why this measure has not been implemented:

SECTION C – DATA BACKUP AND RECOVERY

9) Do you maintain an incident response plan which includes business continuity mitigation procedures in the event of a ransomware threat? ◯ Yes ◯ No

10) Is backup access subject to separate authorization credentials which are maintained separately from common system credentials? ◯ Yes ◯ No

11) Are backup files encrypted? ◯ Yes ◯ No

12) Do you test the successful restoration and recovery of key server configurations and data from backups? ◯ Yes ◯ No

If Yes, how often?

If you answered No to any of the above questions, provide an explanation as to why this measure has not been implemented:

Please include any additional information that may be relevant to the Ransomware Section (optional):

SECTION VI – MEDIA

1) Do you create your own media material or use material provided by others? ◯ Yes ◯ No
   If Yes, please advise:

2) Describe your procedures for removing defamatory, infringing, or damaging materials from your website and mobile applications:

3) Do you send any electronic advertising content to outside parties regarding your products or services or the products or services of your clients? ◯ Yes ◯ No
   If Yes, what media do you use for such advertising?
   - ☐ SMS Text Messaging
   - ☐ Phone Calls
   - ☐ Email
   - ☐ Others:

4) Do you always obtain the appropriate permission from recipients of your advertisements when such permission is required by law? ◯ Yes ◯ No

5) Do your websites allow for others to upload or otherwise share content with others? ◯ Yes ◯ No

SECTION VII – PRIOR CLAIMS AND CIRCUMSTANCES

1) Has any insurer declined, cancelled or non-renewed any similar insurance for which you are applying? ◯ Yes ◯ No
   If Yes, provide complete details:

2) After inquiry, is the applicant, any predecessor, or any other person for whom coverage is requested been subject to any actions or investigations by any regulatory or administrative body for violations arising out of your advertising or electronic communication activities? ◯ Yes ◯ No
   If Yes, provide complete details:

3) After inquiry, is the applicant, any predecessor, or any other person for whom coverage is requested, aware of any actual or alleged fact, circumstance, incident, error or omission that a reasonably prudent person might expect to give rise to a claim or lawsuit whether valid or not, which might directly or indirectly involve the applicant(s), or might give rise to a claim or regulatory proceeding against you? ◯ Yes ◯ No
If Yes, provide complete details:

4) In the past five (5) years:

a. Have any claims suits, or regulatory proceedings been made or brought against you? ◯ Yes ◯ No
If Yes, provide complete details:

b. Have you experienced any:

i. Security incidents, security breaches or cyber-attacks? ◯ Yes ◯ No

ii. Actual or attempted extortion demand with respect to your computer systems? ◯ Yes ◯ No

iii. Unexpected outage of a computer network, application or system lasting greater than four (4) hours? ◯ Yes ◯ No

c. Have you experienced an actual or suspected data breach or cyber-attack? ◯ Yes ◯ No
If Yes, provide a detailed description of the event(s) and remediation action(s) taken:

d. Have you received any complaints concerning the content of your websites or electronic communications? ◯ Yes ◯ No
If Yes, provide complete details:

e. Have you been accused of, made aware of, or had a claim as a result of actual or alleged infringement upon another's domain name, trademark, copyright, services mark or similar intellectual property? ◯ Yes ◯ No
If Yes, provide complete details:

*For each and every claim, click the link to complete the Supplemental Claim Information Form.

Applicable in AL, AR, DC, LA, MD, NM, RI and WV: Any person who knowingly (or willfully)* presents a false or fraudulent claim for payment of a loss or benefit or 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. *Applies in MD only.

Applicable in CO: 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 from insurance proceeds shall be reported to the Colorado Division of Insurance within the Department of Regulatory Agencies.

Applicable in FL and OK: 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)*. * Applies in FL only.

Applicable in KS: 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.

Applicable in KY, NY, OH and PA: 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 (not to exceed five thousand dollars and the stated value of the claim for each such violation)*. *Applies in NY only.

Applicable in ME, TN, VA, and WA: 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 and denial of insurance benefits. *Applies in ME only.

Applicable in NJ: Any person who includes any false or misleading information on an application for an insurance policy is subject to criminal and civil penalties.

Applicable in OR: 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.

Applicable in PR: Any person who knowingly and with the intention of defrauding presents false information in an insurance application, or presents, helps, or causes the presentation of a fraudulent claim for the payment of a loss or any other benefit, or presents more than one claim for the same damage or loss, shall incur a felony and, upon conviction, shall be sanctioned for each violation by a fine of not less than five thousand dollars ($5,000) and not more than ten thousand dollars ($10,000), or a fixed term of imprisonment for three (3) years, or both penalties. Should aggravating circumstances [be] present, the penalty thus established may be increased to a maximum of five (5) years, if extenuating circumstances are present, it may be reduced to a minimum of two (2) years.

Applicable in all other States: 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 material fact, commits a fraudulent insurance act, which is a crime and may also be subject to civil penalty.

I/We understand that this is an application for insurance only and that the completion and submission of this Application does not bind the Company to sell nor the applicant to purchase this insurance. I/We hereby declare that the above statements and particulars are true and I/we agree that this Application shall be the basis for any contract of insurance issued by the Company in response to it.

Electronic Signature of Applicant or Authorized Representative:

Title: Date:

If you prefer not to return the questionnaire with an electronic signature, please print and sign.