

# ADMIRAL TECHNOLOGY PROFESSIONAL LIABILITY APPLICATION AND GENERAL LIABILITY APPLICATION

## SECTION I – INTRODUCTION

1. Full Name of Applicant:  
(Include all prior names, DBAs and subsidiaries seeking coverage under the policy for which you are applying)
  
2. Applicant’s Address (include mailing address if different than physical address):
  
3. Website Address(es):
4. Date Established (mm/dd/yy):
5. FEIN:
6. 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 to either of the above, provide complete details:

## SECTION II – GETTING TO KNOW YOU

7. In your own words, describe your technology services/products:
  
8. Describe the most likely result if your product or service failed to perform as intended:

9. REVENUES:

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

10. Provide the percentage (%) of Total Revenue attributed to foreign locations/operations: %  
 If greater than 0%, provide details including list of countries, number of employees in each and percentage of revenue associated with each country:

11. In the last fiscal year, what percentages of your revenue were from the following services (total should equal 100%):

Software and Hosted Services	Percentage
AI, Generative AI, Machine Learning Software Provider	%
Application Service Provider	%
Automation & Control Systems Software Development, Integration, Sales & Support	%
Cloud Provider / Co-Locating Services	%
Custom Software Development & Licensing	%
GIS / GPS / Mapping / Modeling Software	%
Healthcare Patient Portal – Account Management	%
Managed Service Provider	%
Medical Billing Platform & Other Billing Services	%
Mobile Application Software Development	%
Monitoring (Real Time) Software Development & Sales – No Monitoring or Alert Services	%
Monitoring (Real Time) Software Development & Sales Including Monitoring or Alert Services	%
Payment Processors/Gateway	%
SaaS – Software as a Service Provider	%
Telemedicine Platform & Referral Services	%
<b>Technology Design &amp; Support Services</b>	
Computer Hardware Support	%
Hardware & Software Installation & Integration	%
Technology Consulting – Not Proprietary	%
Technology Product Design & Development for Others – Not Insured’s Proprietary Product	%
Telecommunications System Design, Integration, Consulting	%
Value-Added Reseller of Non-Proprietary Hardware & Software	%
<b>Large Data Services</b>	
Data Aggregation Services	%
Data Destruction Services (Electronic or Physical Data)	%
Electronic Data Storage Services	%
Health Information Exchange	%
<b>Other Services</b>	
Call Center Services	%
Demographic Data & Digital Marketing Consultant	%
Direct Mail & Marketing Distribution Support (Electronic or Physical)	%
Graphic Design, Website Design & Branding Services	%
Internet Service Provider	%
Network Security Consulting & Security Audits (No Real Time Monitoring)	%
Privacy Law based Regulatory Compliance Consulting	%
Technology Staffing	%
Other:	%

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

Type of Clients	Percentage	Type of Clients	Percentage
Aerospace	%	Healthcare	%
Architects, Engineers, Construction	%	Hospitality	%
Automotive	%	Individual Consumers	%
Casino / Gaming	%	Law Enforcement	%
Educational Institutions	%	Manufacturing	%
Energy & Power Generation (Oil, Gas, Solar, Wind, etc.)	%	Retail	%
Entertainment / Athletics	%	Transportation	%
Federal or Local Governments	%	Utilities	%
Financial Institutions	%	Other:	%
		TOTAL:	100%

13. Five largest projects in the last three years?

Client	Services Rendered	Project Duration	Revenue Derived

14. For your Personnel, complete the following breakdown as applicable:

	Number
Technology Development Personnel	
Administrative Personnel	
Sales & Marketing	
Other:	
TOTAL	

15. Do you subcontract any of your services to others?  
If Yes, describe these operations:

Yes No

### SECTION III – TECHNOLOGY RISK MANAGEMENT

(\*Answer all that apply)

16. Is all software development work documented and tested before deployment? Yes No

17. If you host a software application for clients, do you have a secondary backup that can be used in the event of an outage to the application? Yes No

If Yes:

a. Is that back-up stored on an off-site server at a separate location? Yes No

If No, where is the back-up stored?

b. Have you tested the successful restoration of the backup application in the last year? Yes No

- c. Describe any other aspects of your security, testing and recovery procedures around the client environment:
18. If your technology provides real-time monitoring or support, describe the backup procedures in the event of an outage or disruption to the software or technology product the client uses until such outage or disruption is resolved:
19. If you provide any proprietary technology hardware products as part of your offering to clients, complete the following:
- a. Provide the name of the third-party manufacturer of your product:
- b. Describe vetting procedures for selecting the manufacturer:
- c. Do you execute a written contract or agreement with every third-party manufacturer that you use? Yes No
- d. Do you require your third-party manufacturer to carry either or both of the following (check all that apply):
- Professional Liability Insurance
- Commercial General Liability insurance
20. Have any of your products or third-party products you provide to clients been subject to a product recall? Yes No  
If Yes, provide details including product recall costs to you, the remedy and if any third-party claims or litigation related to the product recall:
21. Have you discontinued any software, product, or service in the last five years? Yes No  
If Yes, provide details including whether you continued to provide maintenance and software patching services:

## SECTION IV – NETWORK SECURITY & DATA PRIVACY

### PART 1 – INTERNAL TRAINING, POLICIES AND PROCEDURES

22. Do you conduct employee training on an annual basis (or more frequently) related to:
- a. HIPAA Compliance Yes No
- b. Company Incident Reporting Procedures Yes No
- c. Document Management Yes No
- d. Internet and Email Use Yes No
- e. Passwords Yes No
- f. Responsibility for Company Data Yes No

23. Do you conduct cyber competency testing on an annual basis (or more frequently) for employees and contractors on:
- a. Social engineering attacks (i.e. email-based phishing, baiting, scareware, etc.) Yes No
  - b. Physical security (locked and secured computer devices) Yes No
24. Do you use any of the following technology:
- a. Meta Pixel or similar technology on your website Yes No
  - b. Session Replay or similar technology Yes No
  - c. Chatbot or similar technology Yes No
- If Yes to any of the above, do you request affirmative consent from users? Yes No  
 If No, describe below:

25. Do you have rapid (immediate) account access termination procedures for employees that leave the company? Yes No
26. Do you have a privacy policy? Yes No  
 If Yes, has it been reviewed by legal representation? Yes No
27. Do you maintain an incident response plan which includes business continuity mitigation procedures in the event of a ransomware threat? Yes No

28. a. Are you compliant with the following:

	Indicate N/A, Yes or No			Date of Last Audit/Assessment
Health Information Portability and Accountability Act (HIPAA)	N/A	Yes	No	
Health Information Technology for Economic and Clinical Health Act (HITECH)	N/A	Yes	No	
Payment Card Industry Data Security Standards (PCI DSS)	N/A	Yes	No	

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

c. Complete the chart below for any of the following assessments you have completed:

	Indicate N/A, Yes or No			Date of Last Audit/Assessment
SOC II Certification Type I	N/A	Yes	No	
SOC II Certification Type II	N/A	Yes	No	
Biometric Information Privacy Act (BIPA)	N/A	Yes	No	

d. Describe any changes made to operations, procedures and/or network security and data privacy practices as a result of the recent Audits/Assessments listed in the two charts above:



38. Do you employ Multi-Factor Authentication for the following:

- |   |     |    |
|---|-----|----|
| a. Critical Information                                     | Yes | No |
| b. Remote Access  | Yes | No |
| c. Administrator and privileged user accounts               | Yes | No |
| d. Personal devices accessing the network                   | Yes | No |
| e. Independent contractor and vendors accessing the network | Yes | No |
| f. Non-critical information and applications                | Yes | No |

39. Are workstations prohibited from local admin rights?

Yes No

- |   |     |    |
|---|-----|----|
| a. If Yes, all the time or case by case?  |     |    |
| b. Do you manage privileged accounts using tooling such as CyberArk or other?   | Yes | No |
| c. How many users have persistent privileged accounts for endpoints (defined as those who have entitlements to configure, manage, and support endpoints)? |     |    |

Describe compensating security controls for these specific persistent privileged accounts:

40. Do you route all outbound web requests through a web proxy which monitors for and blocks potentially malicious content?

Yes No

41. Are external emails tagged as such to alert your employees that the email originated from outside of your organization?

Yes No

42. Do you utilize Microsoft Office 365?

Yes No

If Yes, does this include Office 365 Threat Protection add-on?

Yes No

If No, or if you use an alternate product to MS Office 365, provide details or an explanation as to why this measure has not been implemented:

43. Provide the estimated record count of sensitive information you maintain on your servers, store with a cloud provider and host for others:

	Number of Records
Medical Records	
Financial Records (credit/debit cards, bank account #'s, etc.)	
Other Protected Personally Identifiable Information (SSN's, Driver's License #, etc.)	
Biometric Information	
Protected Personally Identifiable Information of Minors	
<b>TOTAL RECORD COUNT</b>	

44. Do you require encryption for the following:

- |  |     |    |
|--|-----|----|
| a. Sensitive information while <u>in transit</u> ? | Yes | No |
| b. Sensitive information while <u>at rest</u> ?    | Yes | No |
| c. Remote Access                                   | Yes | No |

- d. How are your encryption keys protected?
45. 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.
46. How do you ensure sensitive data destruction compliance with applicable privacy law?
47. What are your data security vetting procedures for third parties that you either share data or network access to?
48. 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:

**PART 3 – BACKUP AND RECOVERY**

49. a. How often are network backups performed?
- b. How often are these backups tested?
  - c. Are the backups stored offsite? Yes    No
  - d. Are backup files encrypted? Yes    No
50. Is backup access subject to separate authorization credentials which are maintained separately from common system credentials? Yes    No
51. Do you test the successful restoration and recovery of key server configurations and data from backups? Yes    No  
 If Yes, how often?
52. 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.)*

## PART 4 – CYBER CRIME

53. Is dual authorization required for all wire transfers? Yes No  
If Yes, describe authorization process including which employees or departments have the authority to do so:
54. Are transfer verifications sent to an employee or department other than the one that initiated the transfer? Yes No
55. For employees responsible for wire transfers, is training conducted regarding common wire transfer fraud attack vectors (i.e. social engineering phishing, spear phishing, whaling)? Yes No  
If Yes, how often?
56. Do you call to verify or have another verification process if a client or vendor makes a request via email to change bank account information or key information for future invoices? Yes No  
If Yes, describe:

## SECTION V – MEDIA

57. Do you use media content provided by others? Yes No  
If Yes, describe:
58. Describe your procedures for removing defamatory, infringing, or damaging content from your website and mobile applications:
59. 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:
60. Do you always obtain the appropriate permission from recipients of your advertisements when such permission is required by law? Yes No
61. Do your websites allow for others to upload or otherwise share content with others? Yes No  
If Yes, do you have procedures in place for removing hazardous content? Yes No

## SECTION VI – COVERAGE HISTORY

62. Provide details of your most recent coverage for Professional Liability, Cyber Liability and General Liability. Attach copies of expiring Declarations pages evidencing prior limits and retroactive dates.

	Carrier	Limit	Deductible	Policy Term	Retroactive Date
Professional Liability					
Cyber Liability					
General Liability					

\*If General Liability is purchased, is it on:

Claims Made CGL Form

Occurrence CGL Form

63. Are you interested in a quote for General Liability? Yes No

If Yes, complete the Admiral General Liability Supplement below or submit a signed GL Acord Application.

## SECTION VII – CLAIMS HISTORY

PROVIDE 5 YEARS OF CURRENTLY VALUED LOSS RUNS.

64. Has any insurer declined, cancelled or non-renewed any similar insurance for which you are applying? Yes No

If Yes, provide complete details:

65. 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:

66. Have any claims, suits or regulatory proceedings ever been made against the Applicant or any of its employees? Yes No

If Yes, complete a [Supplemental Claim Information Form](#) for each and every claim.

67. Is the applicant aware of any errors, omissions, circumstances, or incidents which may result in a claim being made against them or their employees, or are there any claims that have not yet been reported? Yes No

If Yes, provide complete details:

68. In the past five (5) years:

a. Have you experienced any:

i. Known intrusions (i.e. unauthorized access), 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 |
| b. Have you experienced an actual or suspected data breach or cyber-attack?<br>If Yes, provide a detailed description of the event(s) and remediation action(s) taken:  | Yes | No |
| c. Have you received any complaints concerning the content of your websites or electronic communications?<br>If Yes, provide complete details:  | Yes | No |
| d. 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?<br>If Yes, provide complete details: | Yes | No |

\*For each and every claim, click the link to complete the [Supplemental Claim Information Form](#).

## **SECTION VIII – COMMENTS**

Use this space below to provide us with any other relevant information:

# GENERAL LIABILITY SUPPLEMENTAL APPLICATION

If you want GL coverage, complete the following or submit a signed GL Acord Application.

## SECTION I – YOUR LOCATIONS

IF YOU HAVE MORE THAN FIVE (5) LOCATIONS, PROVIDE A SPREADSHEET WITH THE INFORMATION BELOW FOR EACH LOCATION.

1.

Loc #	Facility Name	Address	Description / Use	Square Footage	How many other occupants do you share the building with?
1					
2					
3					
4					
5					

## SECTION II – FIRE-LIFE SAFETY INFORMATION

2. Are all of your locations equipped with:

- |   |     |    |
|---|-----|----|
| a. Complete sprinkler system?                       | Yes | No |
| b. At least two clearly marked exits on each floor? | Yes | No |
| c. Smoke detectors?                                 | Yes | No |
| d. Emergency electrical system?                     | Yes | No |
| e. Heat sensors?                                    | Yes | No |
| f. Fire escape(s)?                                  | Yes | No |
| g. Posted emergency evacuation procedures?          | Yes | No |
| h. Properly maintained fire extinguishers?          | Yes | No |

## SECTION III – CLAIMS

PROVIDE 5 YEARS OF CURRENTLY VALUED LOSS RUNS.

- |  |                |        |
|--|----------------|--------|
| 3. Has any General Liability claim or suit been brought against you and/or any of your employees?<br>If Yes, complete a <a href="#">Supplemental Claim Information Form</a> for each and every claim or suit.                        | Yes            | No     |
| 4. Are any persons or entities proposed for this insurance aware of any fact, circumstance, or situation which may result in a GL claim, and has not been reported to your current GL insurance carrier?<br>If Yes, provide details: | None to Report | Yes No |
| 5. Are you aware of any incident, condition, circumstance, defect or suspected defect in any product, which may result in a claim or claims against you that are not listed above?<br>If Yes, provide details:                       | None to Report | Yes No |

**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.**

## Fraud Notices

**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.

**Other State Notices**

**Applicable in RI:** THIS INSURANCE CONTRACT HAS BEEN PLACED WITH AN INSURER NOT LICENSED TO DO BUSINESS IN THE STATE OF RHODE ISLAND BUT APPROVED AS A SURPLUS LINES INSURER. THE INSURER IS NOT A MEMBER OF THE RHODE ISLAND INSURERS INSOLVENCY FUND. SHOULD THE INSURER BECOME INSOLVENT, THE PROTECTION AND BENEFITS OF THE RHODE ISLAND INSURERS INSOLVENCY FUND ARE NOT AVAILABLE.

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.***