

Errors and Omissions, Media, Privacy Application - All States

This is an application for a Claims Made policy. Please read your policy carefully.

INSURANCE OVERVIEW

1. Coverage requested – Please indicate which coverage part(s) are desired and indicate the desired limits. Complete the “Basic Information” section, the “Loss Information” section and any other sections for which coverage is desired.

Coverage Part	Is Coverage Desired?	Limit
A. Professional and Technology Errors and Omissions Liability	<input type="checkbox"/> Yes <input type="checkbox"/> No	\$ _____
B. Media Liability	<input type="checkbox"/> Yes <input type="checkbox"/> No	\$ _____
C. Network Security and Privacy Liability	<input type="checkbox"/> Yes <input type="checkbox"/> No	\$ _____
D. Data Breach Expense Coverage	<input type="checkbox"/> Yes <input type="checkbox"/> No	\$ _____

2. Is similar insurance currently in force? Yes No

Carrier	Limit(s)	Deductible(s)	Premium	Policy Period	Retroactive Date(s):

BASIC INFORMATION

3. Applicant's name: _____
 Location address: _____ Same as mailing address
 City: _____ State: _____ Zip: _____
 Website: _____
 Name of primary contact: _____ Email address of primary contact: _____

4. Description of Operations:

5. Does the applicant provide services not disclosed above or does the applicant anticipate offering any new services in the next 12 months? Yes No

If "Yes," please provide details: _____

6. List 12-month gross revenue below:

	Last Year:	Current Year (based on 12 months):	Forecast for Next Year:
Domestic	\$ _____	\$ _____	\$ _____
Foreign	\$ _____	\$ _____	\$ _____
Total	\$ _____	\$ _____	\$ _____

7. a. Number of principals, partners, officers and employees directly engaged in providing services to clients: _____

b. Number of independent subcontractors: _____

If the applicant uses independent contractors, please answer 7i and 7ii:

i. Do the independent contractors provide the same services as the applicant? Yes No

If "No," please describe services: _____

ii. Does the applicant desire to provide coverage for independent contractors as insureds under the policy? Yes No

If "No," are all independent contractors required to carry errors and omissions insurance? Yes No

8. Describe the three largest jobs or projects over the past three years:

Name of Client	Services Provided	Gross Billings

9. Please provide a breakdown of the applicant's annual revenue by market segment. Please note that the total must equal 100 percent

Market Segment	Percentage (%) of Applicant's Annual Revenue	Market Segment	Percentage (%) of Applicant's Annual Revenue
Aerospace	_____ %	Government (US Federal)	_____ %
Alcohol/Tobacco/Firearms	_____ %	Government (other)	_____ %
Communications	_____ %	Manufacturing/Industrial	_____ %
Construction/Mining/ Agriculture	_____ %	Medical/Health Care Services	_____ %
Education	_____ %	Pharmaceuticals	_____ %
Energy	_____ %	Retail/Wholesale	_____ %
Financial Institutions	_____ %	Transportation	_____ %
Gaming/Gambling	_____ %	Other (please specify): _____	_____ %

10. Date established: _____

11. Does the applicant have any subsidiaries? Yes No

If "Yes," please answer 11a and 11b

a. Name(s) of any subsidiaries: _____

b. Are all subsidiaries' revenue and services disclosed on this application? Yes No

12. a. Is the applicant controlled, owned, affiliated or associated with any other firm, corporation or company? Yes No

b. Is any director, officer or partner either affiliated, employed by or associated with any other firm, corporation or company? Yes No

If "Yes," to either 12a or 12b, please provide name(s) and relationship(s): _____

13. a. Does the applicant derive any revenue from clients for which the applicant is more than a 15 percent shareholder? Yes No

b. Does the applicant derive any revenue from clients for which any director, officer, employee, partner or independent contractor of the applicant serves as an officer or on the board of directors? Yes No

If "Yes," to either 13a or 13b, please provide name(s) and relationship(s): _____

A. PROFESSIONAL AND TECHNOLOGY ERRORS AND OMISSIONS LIABILITY

14. Is the applicant a licensed professional? Yes No

If "Yes," advise type of licensed professional: _____

15. Does the applicant request any additional insureds for professional liability? Yes No

If "Yes," please provide name, address and relationship to applicant: _____

16. How often do you use written contracts: Always Sometimes Never

a. With indemnification clause in favor of you (applicant)? Always Sometimes Never

b. With limitation of damages clauses in favor of you (applicant)? Always Sometimes Never

c. With a clearly defined scope of services to be performed? Always Sometimes Never

d. With a formal change order process with sign-off by both parties? Always Sometimes Never

B. MEDIA LIABILITY

17. Please describe any media activities engaged in by the applicant (including but not limited to publishing, broadcasting, marketing, advertising or otherwise producing or distributing media content):

18. Does the applicant retain a law firm or use in-house counsel to review material for copyright/trademark infringement or personal injury issues? N/A Yes No

If "Yes," please list the name of the firm used (if applicable) and describe review procedures: _____

19. Does the applicant obtain written releases with respect to creative material or talent from employees, models, freelancers, photographers, writers, composers, artists, illustrators, musicians and/or actors? N/A Yes No

20. Are all media materials or advertisements signed off on by clients prior to use? N/A Yes No

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

C & D. NETWORK SECURITY AND PRIVACY LIABILITY/DATA BREACH EXPENSE

22. Does the applicant collect, store or transmit Personally Identifiable Information* in electronic or non-electronic form? Yes No

** Personally Identifiable Information means information concerning an individual that is considered non-public information including but not limited to health, financial or medical information including electronic medical records, social security numbers, financial or bank account information, driver license numbers, credit card numbers and user names and passwords in combination.*

If "Yes," please provide the type(s) and amount of information you process or store. If you do not know the exact amounts, please provide estimates:

Type(s) of Personally Identifiable Information Collected, Transmitted or Stored	Number of Records Collected or Transmitted Per Year	Maximum Number of Records Stored at Any One Time
Social security number or individual taxpayer identification number		
Financial account record (e.g. bank accounts)		
Payment card data (e.g. credit or debit cards)		
Driver's license number, passport number or other state or federal identification number		
Protected health information (e.g. medical records)		
Username/Email address, in combination with password or security question		
Other – Please provide details: _____		

Information/Network Security Risk Management

23. Does the applicant utilize the following controls:

- a. Anti-virus software on all internet accessible devices? Yes No
- b. Firewalls? Yes No
- c. Intrusion detection software? Yes No
- d. Passwords that are non-trivial and contain at least six characters? Yes No
- e. Default passwords changed on all third party hardware and software products? Yes No

24. Does the applicant proactively address system vulnerabilities, including regular updates to anti-virus software and critical security patches? Yes No

25. Has the applicant had a vulnerability assessment, penetration test or other network security assessment performed in the last 12 months? Yes No

If "Yes," please attach a copy.

26. Does the applicant have a data retention and destruction plan in place that includes both electronic and physical data? Yes No

Information/Network Security Policy

27. Does the applicant have a written physical and network security policy in place? Yes No
28. Do all employees receive training on the privacy policy at least annually? Yes No
29. Does the applicant have a designated individual responsible for the management of, and compliance with, the applicant's security policies? Yes No
- If "Yes," what is the name and title of this individual? _____

Breach Response/Disaster Recovery/Business Continuity Planning

30. Does the applicant have a written data breach response plan in place? Yes No
31. Does the applicant back up all valuable/sensitive data on a daily basis? Yes No
- If not daily, how often? _____
32. Does the applicant have a disaster recovery and business continuity plan in place that is designed to avoid business interruption due to IT systems failure? Yes No
- If "Yes":
- a. Is this plan regularly tested and updated? Yes No
- b. How long does it take the applicant to fully restore their systems? _____

Encryption

33. Does the applicant encrypt:
- a. Data "at rest" within computer databases or on back-up storage devices? Yes No
- b. Data "in transit" via email or other electronic means of communication? Yes No
- c. Data stored on mobile devices including laptops, flash drives and mobile phones? Yes No

Physical Security

34. Does the applicant have physical security in place to restrict access to computer systems or paper records that contain sensitive information? Yes No

Employee Controls

35. Does the applicant conduct background checks on all employees? Yes No
36. Does the applicant restrict employee access to Personally Identifiable Information on a business "need-to-know" basis? Yes No
37. Does the applicant have a user revocation process including termination of all passwords and recovery of all data assets when an employee leaves the organization? Yes No
38. Does the applicant provide cyber security training, including social engineering training (e.g. phishing), for employees? Yes No

Cyber Crime

39. What is the applicant's average number of wire transfers per month? _____
40. What is the applicant's average value of wire transfers? _____
41. Does the applicant require dual authorization for wire transfers? Yes No
42. Does the applicant have additional procedures in place to verify the authenticity of wire transfer requests? Yes No
- Please provide details: _____

Third Party Service Providers

43. Does the applicant outsource any part of their network, computer system, data storage (including paper records), point of sale system or information security functions? Yes No
- If "Yes," please provide details including the functions outsourced and the names of the vendors used: _____
- _____
44. Does the applicant require third party providers to have minimum security measures for the use, storage and disclosure of Personally Identifiable Information shared between them and the applicant? Yes No

Privacy

45. Does the applicant rent, sell or otherwise share any Personally Identifiable Information with third parties? Yes No

Regulatory Compliance

46. If the applicant provides services that are involved in credit card or other payment card transactions, is the applicant compliant with Payment Card Industry Data Security Standards (PCI DSS)? N/A Yes No

If "No," please explain: _____

47. If the applicant provides services that involve medical records or patient data of any kind, is the applicant compliant with the Health Information Portability and Accountability Act (HIPAA)? N/A Yes No

If "No," please explain: _____

48. Is the applicant subject to any other regulations that pertain to the protection of private or personal information? Yes No

If "Yes," please list the name of the applicable regulation(s) and confirm the applicant is fully compliant with such regulation(s):

LOSS INFORMATION

(Attach a statement of details for all "Yes" answers to the following questions)

49. Has any prospective insured ever had their license revoked or suspended, been fined or disciplined in any way or been the subject of any investigation by any regulating body related to their profession? Yes No

50. Have you initiated litigation against any of your clients in the past five years? Yes No

51. During the past five years, has any claim been made or suit brought against the applicant, its predecessor(s) in business or any of its present or former owners, partners, officers, directors, employees or independent contractors? Yes No

52. Is any owner, partner, officer, director, employee or independent contractor aware of any circumstance, allegation, contention or incident which may result in a claim being made against the applicant, its predecessor(s) in business or any of its present or former partners, owners, officers, directors, employees or independent contractors? Yes No

53. Has any policy or application for professional liability insurance on your behalf or on the behalf of any of your principals, officers, employees, independent contractors or on behalf of any predecessor(s) in business ever been declined, cancelled or renewal refused? (Not applicable in Missouri) Yes No

54. Has any regulatory, governmental or administrative action(s) been brought against the applicant involving actual or alleged privacy violations, including but not limited to the use or disclosure of Personally Identifiable Information? Yes No

55. Is the applicant aware of any data breach or security breach (including a ransomware incident) that has or may result in unauthorized use or disclosure of personally identifiable information or other private information held by the applicant or held by a client of the applicant? Yes No

56. Has the applicant received or are they aware of any complaint, notice or claim involving a data breach resulting in the unauthorized use or disclosure of Personally Identifiable Information held by the applicant or Personally Identifiable Information held by a client of the applicant? Yes No

57. Has the applicant experienced a loss of funds or goods resulting from social engineering fraud, telecommunications fraud, or wire transfer fraud in the past five years? Yes No

58. In the last five years, has there been an unplanned outage of the applicant's network or computer systems lasting more than eight hours? Yes No

FRAUD STATEMENTS

Alabama, Arkansas, District of Columbia, New Mexico, Rhode Island and 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 Fraud Statement: 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.

Florida Fraud Statement: 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 Fraud Statement: 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.

Maine Fraud Statement: 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 a denial of insurance benefits

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

New York Fraud Statement: 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.

Oklahoma Fraud Statement: 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 Fraud Statement: Notice to Oregon applicants: 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 may be guilty of insurance fraud.

Kentucky, Pennsylvania AND Ohio Fraud Statement: 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.

Tennessee, Virginia and Washington Fraud Statement: 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.

Fraud Statement (All Other States): 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 may be guilty of a crime and may be subject to fines and confinement in prison.

STATE NOTICES

Arizona Notice: Misrepresentations, omissions, concealment of facts and incorrect statements shall prevent recovery under the policy only if the misrepresentations, omissions, concealment of facts or incorrect statements are; fraudulent or material either to the acceptance of the risk, or to the hazard assumed by the insurer or the insurer in good faith would either not have issued the policy, or would not have issued a policy in as large an amount, or would not have provided coverage with respect to the hazard resulting in the loss, if the true facts had been made known to the insurer as required either by the application for the policy or otherwise.

Florida Surplus Lines Notice: (Applies only if policy is non-admitted) You are agreeing to place coverage in the surplus lines market. Superior coverage may be available in the admitted market and at a lesser cost. Persons insured by surplus lines carriers are not protected under the Florida Insurance Guaranty Act with respect to any right of recovery for the obligation of an insolvent unlicensed insurer.

Florida and Illinois Punitive Damage Notice: I understand that there is no coverage for punitive damages assessed directly against an insured under Florida and Illinois law. However, I also understand that punitive damages that are not assessed directly against an insured, also known as "vicariously assessed punitive damages", are insurable under Florida and Illinois law. Therefore, if any Policy is issued to the applicant as a result of this Application and such Policy provides coverage for punitive damages, I understand and acknowledge that the coverage for Claims brought in the State of Florida and Illinois is limited to "vicariously assessed punitive damages" and that there is no coverage for directly assessed punitive damages.

Maine Notice: The insurer is not permitted to withdraw any binder once issued, but a prospective notice of cancellation may be sent and coverage denied for fraud or material misrepresentation in obtaining coverage. A policy may not be unilaterally rescinded or voided.

Ohio Representation Statement: By acceptance of this policy, the Insured agrees the statements in the application (new or renewal) submitted to the company are true and correct. It is understood and agreed that, to the extent permitted by law, the Company reserves the right to rescind this policy, or any coverage provided herein, for material misrepresentations made by the Insured. It is understood and agreed that the statements made in the insurance applications are incorporated into, and shall form part of, this policy. **THE INSURED UNDERSTANDS AND AGREES THAT ANY MATERIAL MISREPRESENTATION OR OMISSION ON THIS APPLICATION WILL ACT TO RENDER ANY CONTRACT OF INSURANCE NULL AND WITHOUT EFFECT OR PROVIDE THE COMPANY THE RIGHT TO RESCIND IT.**

Utah Punitive Damages Notice: I understand that Punitive Damages are not insurable in the state of Utah. There will be no coverage afforded for Punitive Damages for any Claim brought in the State of Utah. Any coverage for Punitive Damages will only apply if a Claim is filed in a state which allows punitive or exemplary damages to be insurable. This may apply if a Claim is brought in another state by a subsidiary or additional location(s) of the Named Insured, outside the state of Utah, for which coverage is sought under the same policy.

If your state requires that we have information regarding your Authorized Retail Agent or Broker, please provide below.

Retail agency name: _____ License #: _____

Agent's signature: _____ Main agency phone number: _____

(Required in New Hampshire)

Agency mailing address: _____

City: _____ State: _____ Zip _____

The signer of this application acknowledges and understands that the information provided in this Application is material to the Insurer's decision to provide the requested insurance and is relied on by the Insurer in providing such insurance. The signer of this application represents that the information provided in this Application is true and correct in all matters. The signer of this Application further represents that any changes in matters inquired about in this Application occurring prior to the effective date of coverage, which render the information provided herein untrue, incorrect or inaccurate in any way will be reported to the Insurer immediately in writing. The Insurer reserves the right to modify or withdraw any quote or binder issued if such changes are material to the insurability or premium charged, based on the Insurer's underwriting guides. The Insurer is hereby authorized, but not required, to make any investigation and inquiry in connection with the information, statements and disclosures provided in this Application. The decision of the Insurer not to make or to limit any investigation or inquiry shall not be deemed a waiver of any rights by the Insurer and shall not estop the Insurer from relying on any statement in this Application in the event the Policy is issued. It is agreed that this Application shall be the basis of the contract should a policy be issued and it will be attached and become a part of the Policy.

Applicant's signature: _____ Title: _____

(President, Owner, Partner, Chairperson of the Board, Managing Member, Executive Director or Executive Officer)

Date: _____

Errors and Omissions, Media and Privacy (EMP)

Claims Examples



Errors and Omissions

A management consulting firm specializing in efficiency consulting was hired to reduce the cost of distribution for a large chain of retail bakeries. They advised the company to concentrate on baking and packaging and to contract out delivery to a trucking company. The consulting firm worked closely with the bakery to complete the changes by the end of their fiscal year. Delays in contract negotiation with the trucking company caused distribution setbacks for the company's flagship product, Independence Day-themed cupcakes. The cupcakes did not arrive in time for the holiday, causing the bakery a significant loss in revenue. The management consultant was sued for negligence and defense costs exceeded \$200,000.

Technology Errors and Omissions

A software company was hired by a transportation company to design a software program that would route freight more efficiently. After six months, the developer failed to deliver the program as promised in their contract, and the company was forced to hire a replacement firm to complete the project. The transportation company sued for damages of \$3,000,000, which included the additional cost to complete the program and recover lost profits. The software company argued damages sustained by the plaintiff were limited to \$650,000 in fees paid for the software program. However, due to the negligence of the software design firm, the jury rendered a verdict of over \$1,000,000 in favor of the plaintiff.

Intellectual Property

During a televised sporting event, a car company aired a commercial that showed a ball with a trademark symbol bearing a striking resemblance to a logo of a luxury fashion designer. The fashion designer filed suit against the car company alleging trademark violations. It turned out that neither the car company nor their ad agency had permission to use the trademark. The fashion designer won summary judgment in the case and was ultimately awarded damages of \$3,200,000.

Cyber Crime

A fulfillment company employee gets an email from who they thought was their CFO asking them to wire money to a bank to pay for packing materials. Unfortunately, it was a spear phishing email and the money was wired to an unknown account that was quickly closed after receiving the funds. The amount lost totaled over \$100,000.

Network Security and Privacy Liability

An employee of a marketing company inadvertently downloaded a destructive virus that quickly spread throughout their network. As a result, approximately 25 percent of the company's customers were infected with the same virus. Consequently, their customers suffered a widespread loss of data and a complete shutdown of their networks. The customers filed a class action suit against the company, claiming they should have prevented the transmission of the virus. The customers sought damages for the cost to restore lost data and their economic loss. Total damages awarded were over \$3,000,000.

Regulatory Defense

A national network support company has field employees who frequently used company-issued laptops at customer locations. The laptops contained sensitive data from their customers' networks, including social security numbers and medical records. One day, an employee of the support company had his laptop stolen from his car. Although the data on his laptop was encrypted, the employee had his password taped to the laptop. Due to embarrassment, the employee did not notify the employer until two months later. Although the network support company immediately set about notifying affected parties of the breach, they were ultimately fined by the Attorney General for not notifying their customers in the time frame allotted by the state. The total amount of loss and claim expense was over \$700,000.

Payment Card Industry (PCI) Fines and Penalties

A cloud content provider was notified by its payment card-processing bank of a possible data breach to their payment system. A forensic investigation found that the content company unknowingly transmitted unencrypted credit card numbers. The payment card processor demanded indemnification for fines assessed by the credit card companies who alleged a data breach. The payment card processor withdrew \$100,000 from the content company's bank account and sued them for the balance of \$500,000.

Privacy Breach Expense

A fulfillment service was hit with a data breach that exposed the credit and debit card numbers and expiration dates of approximately 480,000 customers. The company spent over \$890,000 to hire a firm to conduct forensics to determine all those affected, re-secure its network and send out notification letters across multiple states. They also set up credit monitoring for its customers and spent an additional \$90,000 on hiring a public relations firm to manage the publicity surrounding the event. The costs associated with the breach were over \$1,000,000.

Cyber Extortion Threat Expense

The owner of a marketing agency arrived at the office to discover he and his employees were locked out of their computer system. A hacker notified him that the agency had 48 hours to pay \$50,000 or all files on their server would be deleted. As the deadline approached, the owner realized that he couldn't thwart the attack and was forced to pay the amount demanded.



Email submissions to professional@devonparkspecialty.com

This document does not amend, extend or alter the coverage afforded by the policy. For a complete understanding of any insurance you purchase, you must first read your policy, declaration page and any endorsements and discuss them with your agent. A sample policy is available from your agent. Your actual policy conditions may be amended by endorsement or affected by state laws.