

Smart Tech Errors & Omissions Insurance™ Application

1. Company Name

2. Company Address

3a. Primary Website¹

3b. Additional Websites

4. Does the Applicant currently have similar coverage in place?

Yes

No

5. Are there any subsidiaries for which the Named Insured wishes to cover under the policy? If yes, please list the names below and provide a relevant organization chart.

Yes

No

6. Current Gross Annual Revenue (Previous 12 months).

7. Projected Gross Annual Revenue (next 12 months).

8. Estimated amount of unique personally identifiable records² stored, processed or transmitted by the Applicant (including records stored by third-party providers).

0 - 250,000

500,001 - 1,000,000

2,500,001 - 5,000,000

10,000,001 +

250,001 - 500,000

1,000,001 - 2,500,000

5,000,001 - 10,000,000

Description of technology products/services offered for others for a fee or other compensation or consideration.

10. Please provide a breakout of the percentage of revenue derived from the products/services listed below:

<input type="text"/>	Application service provider / Software as a Service	<input type="text"/>	Mobile Application Development
<input type="text"/>	Audio Visual Implementation / Consulting	<input type="text"/>	Network Security Software and Services
<input type="text"/>	Cloud Computing (including servers, storage, databases, networking, software, analytics, and intelligence)	<input type="text"/>	Payment Processing for others for a fee
<input type="text"/>	Cryptocurrency / Blockchain Software Services	<input type="text"/>	Software Development, Installation, and/or Training - Custom
<input type="text"/>	Data and Transaction Processing/Analytics	<input type="text"/>	Software Development, Installation, and/or Training - Prepackaged
<input type="text"/>	Data Management Service Provider	<input type="text"/>	Technical Support / Repair / Maintenance
<input type="text"/>	Digital Advertising / Search Engine Optimization / Lead Generation Software	<input type="text"/>	Telecommunication Services
<input type="text"/>	E-Cycling / Document Management / Shredding	<input type="text"/>	Telemedicine Services
<input type="text"/>	Hardware Manufacturing	<input type="text"/>	Technology hardware/equipment sales and maintenance (including robotics)
<input type="text"/>	Internet Service Provider	<input type="text"/>	Value Added Software Resale, Installation, Integration
<input type="text"/>	IT Business Process Outsourcing Services	<input type="text"/>	Website Hosting and Colocation Services
<input type="text"/>	IT Consulting	<input type="text"/>	Website Design, Consulting, Development
<input type="text"/>	IT Staffing Services	<input type="text"/>	OTHER: Please provide details below:
<input type="text"/>	Managed IT Services (including MSP and MSSP services)	<input type="text"/>	

11. Please list the Applicant's 3 largest contracts including client name and annual value of the contract:

Client Name	Annual Value (USD)
<input type="text"/>	<input type="text"/>
<input type="text"/>	<input type="text"/>
<input type="text"/>	<input type="text"/>

12. Does the Applicant always utilize written contracts with customers?	Yes	No
13. Does legal counsel approve all changes to standard contracts?	Yes	No
14. Does the Applicant require customer acceptance or sign-off within agreements or contracts?	Yes	No
15. Does the Applicant require a Hold Harmless clause benefiting the Applicant within agreements or contracts?	Yes	No
16. Does the Applicant require Limitation of Liability within agreements or contracts?	Yes	No
17. Does the Applicant include a waiver of implied warranty or any other warranty, except explicit warranties, to the extent allowable by law?	Yes	No
18. Does the Applicant include exclusion of consequential damages in their contracts inuring to their benefit?	Yes	No
19. Prior to executing an electronic payment, does the Applicant verify the validity of the funds transfer request or payment change request, with the requestor ³ , via a separate means of communication prior to transferring funds or making payment changes?	Yes	No

20. How often do you conduct security training or phishing training for employees, executives, and key accounting personnel?

- | | | |
|------------------|----------------------|-------------------------------|
| Ad-hoc | Semi-Annually | Never |
| Quarterly | Annually | Yes, frequency unknown |

21. Do you have email filtering in place?

Yes

No

If "Yes", list the name of your email filtering solution.

Do you use an advanced email security solution that includes features such as URL and attachment sandboxing. (Secure Email Gateway)

Yes

No

If "Yes", please list the name of your solution.

22. Do you have a backup solution?

Yes

No

If "Yes", how frequently do you back up systems and data?

Continuous backups

Weekly

Less than monthly

Daily

Monthly

Never

23. Which of the following are in place for your backup solution(s)?

Backup servers are segmented from the rest of the network

Copy of backups are kept offline or air-gapped

Cloud based backups

Multiple copies of backups stored in 2 or more geographical locations

MFA required for access to backups files (on-premise and cloud)

Backup solution with immutable backups

Backup servers are not joined to a Windows domain

Backup servers and user accounts leverage unique credentials

Backups are encrypted

Other Controls (Describe your current backup process and solution):

24. Do you enforce Multi-Factor Authentication to secure all remote access to your network? Yes No N/A

25. Do you enforce Multi-Factor Authentication to secure and manage internal use of privileged accounts (administrator accounts, service accounts, etc.)? Yes No

26. Do you enforce Multi-Factor Authentication (MFA) for email access via webmail portal (i.e. Gmail), mailbox applications (i.e. Outlook Application) and non-corporate devices for all employees? Yes No

27. What Endpoint Security Technology do you have in place? (check all that apply)

Standard Antivirus

Next Gen Antivirus

Endpoint Protection (EPP) across your enterprises

Endpoint Protection & Response (EDR) across your enterprises

Managed Detection & Response (MDR) across your enterprises

Extended Detection & Response (XDR) across your enterprises

28. Do you have a Business Continuity Plan (BCP) or Disaster Recovery Plan (DRP) in place? Yes No

29. In the event of an interruption of the Applicant’s network, what is the Applicants recovery time objective for critical systems, applications and processes?

≤ 10 hours

≤ 24 hours

≤ 12 hours

Greater than 24 hours

30. How is sensitive data encrypted across systems and devices? (check all that apply)

No encryption

Full disk encryption (laptops)

Mobile Device encryption (eg cell phones, laptops, etc.)

Full disk encryption (workstations, on-premise laptops, etc.)

Encryption at Rest (File Level) File level encryption

Encryption of Data in-transit

Other encryption methods

31. If the Applicant accepts payment cards in exchange for goods or services rendered, is the Applicant or their outsourced payment processor PCI compliant⁴?

Yes

No

N/A

32. If the Applicant uses multimedia material provided by others, does the Applicant always obtain the necessary rights, licenses, releases, and consents prior to publishing?

Yes

No

N/A

33. Has the Applicant ever experienced any technology services or professional services errors or omissions, cyber security, data privacy, electronic crime/social engineering, or multimedia liability⁵ incidents in the past three years?

Yes

No

If Yes: Please provide additional details.

34. Does the Applicant or any other person or organization proposed for this insurance have knowledge of any technology errors or omissions, security breach, privacy breach, privacy-related event or incident or allegations of breach of privacy that may give rise to a claim?

Yes

No

If Yes: Please provide additional details.

35. Has the Applicant or any other organization proposed for this insurance sustained any unscheduled network outage or interruption lasting longer than six hours within the past three years?

Yes

No

If Yes: Please provide additional details.

37. Additional Notes

Applicant Signature

Print Name

Date

Applicant Email⁶ (optional)

Applicant Title (optional)

Footnotes

¹ Corvus runs a scan on the Applicant's primary corporate website and any affiliated sites in order to create our Dynamic Loss Prevention report. We include the high-level results of the scan in our quote along with a preview of several personalized recommendations for the Applicant. After the Applicant binds a quote, Corvus generates a full report detailing the results of the scan, including all of our personalized recommendations for the Applicant.

² PII includes any information that can be used to distinguish or trace an individual's identity, either alone or when combined with other personal or identifying information that is linked or linkable to a specific individual.

³ A secondary verification method with the requestor of a funds transfer through a communication channel separate from the original request.

⁴ PCI is an information security standard for organizations that handle branded credit cards from the major credit card brands.

⁵ A multimedia liability claim includes one alleging defamation, disparagement, invasion of privacy, commercial misappropriation of likeness, plagiarism, piracy, or copyright or trademark infringement.

⁶ You will be added to our software platform, the CrowBar, which provides helpful risk management advice, alerts and services.

Notices

Notice to All Applicants: 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, for the purpose of misleading, conceals information concerning any fact material thereto, may commit a fraudulent insurance act which is a crime and subjects such person to criminal and civil penalties in many states.

Notice to Colorado Applicants: 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 claiming 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.

Notice to District of Columbia and Louisiana Applicants: 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.

Notice to Florida Applicants: Any person who knowingly and with intent to injure, defraud or deceive any insurance company, files a statement of claim containing any false, incomplete, or misleading information is guilty of a felony of the third degree.

Notice to Oklahoma Applicants: Any person who knowingly, and with intent to injure, defraud or deceive any insurer, files a statement of claim containing any false, incomplete or misleading information is guilty of a felony.

Notice to Kansas Applicants: An act committed by 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.

Notice to Maine, Tennessee, Virginia and Washington Applicants: 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/or denial of insurance benefits.

Notice to Maryland Applicants: 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.

Notice to New Hampshire Applicants: Any person who, with a purpose to injure, defraud or deceive an insurance company, files a statement of claim containing any false, incomplete or misleading information is subject to prosecution and punishment for insurance fraud as provided in RSA 638:20.

Notice to New York Applicants: 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 \$5,000 and the stated value of the claim for each such violation.

Notice to Pennsylvania Applicants: 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 purposes 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.