DUAL Tech-Cyber-Media Insurance Application (9-12-23 Edition)

Please answer all the following questions on this form. Before any question is answered please carefully read the declaration at the end of the application form, which you are required to sign. Underwriters will rely on the statements that you make on this form. PLEASE TAKE CARE IN FILLING OUT THIS FORM.

# General Information

1.) Name of Applicant

Address

City State Zip

Total Number of Employees Website

2.) Please provide your NAICS 6-digit code (if available)

3.) Most recent fiscal year revenue Year ending

4.) From the following choices, please select all of which best describe your business (Up to 100% of total revenue indicated above):

|  |  |  |  |
| --- | --- | --- | --- |
| **Business Service/Product Offered** | **% of**  **Revenue** | **Business Service/Product Offered** | **% of**  **Revenue** |
| Software/Hardware Reseller  (3rd party products only) |  | Website Hosting Services |  |
| Network/Systems Consulting  Services (3rd party products only) |  | Data Hosting and Co-location  Services and Products |  |
| Website & Graphic Design and  Advertising Services |  | Network/Systems Security  Software/Hardware Development |  |
| E-Commerce or Online Retailer |  | Educational Software/Hardware  Development |  |
| Application Service Provider (ASP) or Managed Software-as-a-Service  (SAAS) |  | Network/Systems Security Consulting Services (3rd party  products only) |  |
| Enterprise Resource Planning (ERP) or Business Process  Software Development |  | Telecommunications Consulting & Installation Services (3rd party  products only) |  |
| Mobile Application Software  Development (Non-Gaming) |  | Video Game and Mobile Game  Software/Hardware Development |  |
| Robotics and Automation Software  Hardware Development |  | Managed Service or Infrastructure  as a Service Provider |  |
| Internet Service Provider (1st party Services and Products) |  | Other: |  |

# Technology Professional Services Information

5.) Do you secure an executed contract agreement with all your clients? Yes No\*

\*If No, % of total clients with contracts? %

6.) Please identify any of the following risk mitigating clauses contained in your standard contract agreement with clients:

|  |  |  |
| --- | --- | --- |
|  | Client Acceptance/Final Sign Off?  Force Majeure? Limitation of Liability?  Exclusion of Consequential Damages? Hold Harmless Agreements?  Payment Terms? Disclaimer of Warranties? Indemnification Clauses? Project Milestones? | Yes  Yes Yes Yes Yes Yes Yes Yes Yes |
| 7.) | Do you have a formal recall process in place? | Yes No |
| 8.) | Do you sell, distribute or develop software bound by an open source? | Yes\* No |
|  | \*If Yes, do you ensure that all software code is used in compliance with applicable free software or open source code license standard practices? | Yes No |
| 9.) | Do you sell, distribute or develop software bound by a 3rd party license? | Yes\* No |
|  | \*If Yes, do you ensure that all software code is used in compliance with the 3rd party license agreement and take added steps to mitigate an intellectual property claim? | Yes No |

10.)Are you audited on, at least, a yearly basis for SSAE 18 (or SOC 2 if

applicable) and are compliant? Yes No

11.)Does your hiring process include criminal background checks? Yes No

# Network Security Information

12.)Approximate number of Personally Identifiable Individuals (PII\*) records that are retained within your computer network, systems, databases and file records?

\*PII is defined as a personally identifiable record on a person that can be used to identify, contact or locate a single individual. Please see Question #6 below.

13.)Please identify the type of PII retained on your network:

Payment Card Data? Yes No

Personnel Records? Yes No

Health Care Records? Yes No

Drivers License Numbers? Yes No

Social Security Numbers? Yes No

Home Address? Yes No

14.)If you process or store payment card data, are you PCI-DSS Compliant? Yes No

15.)Are staff with access to your network trained and assessed in privacy and security

Related matters such as phishing, social engineering, social media and identity theft? Yes No

16.)Do you have company-wide policy that addresses compliance with privacy and security laws or regulations as required for your business, industry or required by

jurisdiction where it conducts business and are they reviewed by a qualified attorney or

third party and updated as required? Yes No

17.)Do you have firewalls in force across your network? Yes No

18.)Do you have anti-virus software in force across your network including all desktops, laptops, servers (excluding database servers); and is the anti-virus software updated on,

at least, a monthly basis? Yes No

19.)Do you use any endpoint malware detection software such as Carbon Black, AMP,

Sophos, Falcon, EDR or Defender? Yes No

20.)Does your company policy require multi-factor authentication for all user remote access

to company systems and networks? Yes No

21.)Do you or your email provider scan all incoming emails for malicious links and

attachments? Yes No

22.)Do you have a written Incident Recovery or Business Continuity plan in force for

network security incidents and network outages? Yes No

23.)Do you back-up your computer system and network data on, at least, a weekly basis? Yes No

24.)Are computer system and network data backups stored in either an offsite or offline

location with no logical connection to your main operating systems? Yes No

25.)Do you test the implementations of your computer system and network data

backups on at least a quarterly basis? If not quarterly, then how often? Yes No

26.)Is all sensitive and confidential information, including PII, stored on your networks,

systems and databases encrypted? Yes No

27.) Are all company portable and mobile devices encrypted? Yes No N/A\*

\*Please select N/A if either you do not have company mobile devices and/or it is company policy not to store sensitive and confidential information on these devices.

28.)If you have answered ‘No’ to question #27 above, please provide us with details regarding the type of sensitive/confidential information stored on these devices and compensating controls in place to ensure a breach does not occur.

.

29.)Do you have a process in force to obtain a legal review of all media and advertising

content prior to release? Yes No

30.)Does the Applicant use any vendors for Managed Security, Cloud, Back-up, Website hosting, Internet Service, Business Software, Data Processing or Payment/Point-of-Sale

Providers? Yes \* No

\*If Yes, please list ALL vendor names:

.

# Media Information

31.)Do you have a formal media and content clearance procedure in place? Yes No

32.)Please identify any of the following risk mitigating clauses contained in your media and content clearance procedures:

Acquisition of all necessary 3rd party content licenses, rights and consents? Yes Process to handle complaints regarding content released? Yes

Training of employees in regards to copyright and trademark issues? Yes

Intellectual Property Audits conducted by legal counsel? Yes Screening of media and takedown procedures for disparaging, libelous or

slanderous content? Yes

33.)Are you compliant with the Digital Millennium Copyright Act or equivalent? Yes No

# Historical Information

34.)Have you ever had any products recalled? Yes No

35.)Have you sustained any network intrusion, corruption, breach or loss of data in past 3

years? Yes No

36.)Have you received any injunction(s), lawsuit(s), fine(s), penalty(s), sanction(s), or been subject to any regulatory, administrative action or investigation pertaining to the type of

insuring being requested on this Application in the past 3 years? Yes No

37.)Are you aware of any circumstance or incident that could be reasonably anticipated to give rise to a claim pertaining to the type of insurance being requested on this

Application? Yes No

# Data Protection

By accepting this insurance you consent to DUAL Commercial using the information we may hold about you for the purpose of providing insurance and handling claims, if any, and to process sensitive personal data about you where this is necessary (for example health information or criminal convictions). This may mean we have to give some details to third parties involved in providing insurance cover. These may include insurance carriers, third party claims adjusters, fraud detection and prevention services, reinsurance companies and insurance regulatory authorities.

Where such sensitive personal information relates to anyone other than you, you must obtain the explicit consent of the person to whom the information relates both to the disclosure of such information to us and its use by us as set out above. The information provided will be treated in confidence and in compliance with relevant Data Protection legislation. You have the right to apply for a copy of your information (for which we may charge a small fee) and to have any inaccuracies corrected.

# IMPORTANT – Tech Cyber Media Policy Statement of Fact

By accepting this insurance, you confirm that the facts contained in the supplemental application form are true. These statements, and all information you or anyone on your behalf provided before we agree to insure you, are incorporated into and form the basis of your policy. If anything in these statements is not correct, we will be entitled to treat this insurance as if it had never existed. You should keep this Statement of Fact and a copy of the completed proposal form for your records.

This application must be signed by the applicant. Signing this form does not bind the company to complete the insurance. With reference to risks being applied for in the United States, please note that in certain states, any person who knowingly and with intent to defraud any insurance company or other person submits an application for insurance containing any false information, or conceals the purpose of misleading information concerning any fact material thereto, commits a fraudulent insurance act, which is a crime.

The undersigned is an authorized principal, partner, director, risk manager, or employee of the applicant and certifies that reasonable inquiry has been made to obtain the answers herein which are true, correct and complete to the best of his/her knowledge and belief. Such reasonable inquiry includes all necessary inquiries to fellow principals, partners, directors, risk managers, or employees to enable you to answer the questions accurately.

Name

Sign

Date