DUAL Cybersecurity insurance application

(10-13-2020 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.

1. Name of applicant:			
Address:			
City	**State**		**Zip**
Total number of employees	**Website**		
2. From the following choices, please select which best describes your business:			
Manufacturer, Construction, Architect or Engineer?		Yes	No
Other?		Yes	No
3. Please provide your NAICS 6-digit code (if available)			
4. Most recent fiscal year revenue		**Year ending**	
5. Approximate number of Personally Identifiable Individuals (PII*) records 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.			
6. Please identify the type of PII retained on your network:		Yes	No
Payment card data?		Yes	No
Personnel records?		Yes	No
Health care records?		Yes	No
Driver's license numbers?		Yes	No
Social security numbers?		Yes	No
Home address?		Yes	No
7. If you process or store payment card data, are you PCI-DSS Compliant?		Yes	No

8. 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	
9. 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	
10. Do you have firewalls in force across your network?	Yes	No	
11. 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	
12. Do you use any endpoint malware detection software such as Carbon Black, AMP, Sophos, Falcon, EDR or Defender?	Yes	No	
13. Do you use multi-factor authentication for all user access to company systems and networks?	Yes	No	
14. Do you or your email provider scan all incoming emails for malicious links and attachments?	Yes	No	
15. Do you have a written Incident Recovery or Business Continuity plan in force for network security incidents and network outages?	Yes	No	
16. Do you back-up your computer system and network data on, at least, a weekly basis?	Yes	No	
17. Are computer system and network data backups stored in either an offsite or offline location with no connection to your main operating systems?	Yes	No	
18. 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	
19. Is all sensitive and confidential information, including PII, stored on your networks, systems and databases encrypted?	Yes	No	
20. Are all company portable and mobile devices encrypted? ***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.**	Yes	No	N/A*
21. If you have answered 'No' to question #20 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.		
22.	**Do you have a process in force to obtain a legal review of all media and advertising content prior to release?**	Yes	No
23.	**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?** If Yes, please list ALL vendor names:	Yes	No
24.	**Have you sustained any network intrusion, corruption, breach or loss of data in past 3 years?**		
25.	**Have you received any privacy related injunction(s), lawsuit(s), fine(s), penalty(s), sanction(s), or been subject to any privacy regulatory, administrative action or investigation in past 3 years?**	Yes	No
26.	**Are you aware of any circumstance or incident that could be reasonably anticipated to give rise to a claim against the type of insurance being requested on this Cyber Security Application?**	Yes	No

Data protection

By accepting this insurance, you consent to DUAL North America 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 – Cybersecurity 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	
Signature	
Date	