

Cyber Liability and Breach Response Coverage Increased Limits Request Form

Please fully answer all questions and submit all requested information.

I. GENERAL INFORMATION

Full Name:			
Mailing Address:		State of Incorporation:	
City:		State & Zip:	
# of Employees:		Date Established:	
Website URL's:			
Authorized Officer 1:		Telephone:	
		E-mail:	
Breach Response Contact ² :		Telephone:	
		E-mail:	
Business Description:			
Does the Applicant provide data processing, storage or hosting services to third parties?			<input type="checkbox"/> Yes <input type="checkbox"/> No

II. REVENUE INFORMATION

Provide Gross Revenue information

	Most Recent Twelve (12) months: (ending: ____/____)	Previous Year	Next Year (estimate)
US Revenue:	USD	USD	USD
Non-US Revenue:	USD	USD	USD
Total:	USD	USD	USD

Please attach a copy of your most recently audited annual financial statement.

¹ This is the officer of the Applicant that is authorized make statements to the Underwriters on the Applicant's behalf and to receive notices from the Insurer or its authorized representative(s).

² This is the employee of the Applicant that is designated to work with the insurer in response to a data breach event.

What percentage of the Applicant's revenues are business to business?	%
Direct to consumer?	%
Are significant changes in the nature or size of the Applicants business anticipated over the next twelve (12) months? Or have there been any such changes within the past twelve (12) months?	<input type="checkbox"/> Yes <input type="checkbox"/> No
If Yes, please explain:	
Has the Applicant within the past twelve (12) months completed or agreed to, or does it contemplate entering into within the next twelve (12) months, a merger, acquisition, consolidation, whether or not such transactions were or will be completed?	<input type="checkbox"/> Yes <input type="checkbox"/> No
If Yes, please explain:	

III. PRIVACY AND COMPUTER & NETWORK SECURITY

Does the Applicant have and require employees to follow written computer and information systems policies and procedures?	<input type="checkbox"/> Yes <input type="checkbox"/> No
Does the Applicant use the following controls:	
Commercially available Firewall protection:	<input type="checkbox"/> Yes <input type="checkbox"/> No
Commercially available Anti-Virus protection:	<input type="checkbox"/> Yes <input type="checkbox"/> No
If No, Please describe the alternative controls implemented to prevent unauthorized access or intrusion to Computer Systems:	
Does the Applicant terminate all computer access and user accounts as part of the regular exit process when an employee leaves the company or when a third party contractor no longer provides the contracted services?	<input type="checkbox"/> Yes <input type="checkbox"/> No
Does the Applicant accept credit cards for goods sold or services rendered?	<input type="checkbox"/> Yes <input type="checkbox"/> No
If Yes,	
Please state the Applicants approximate percentage of revenues from credit card transactions within the past twelve (12) months:	%
Is the Applicant compliant with applicable data security standards issued by financial institutions with which the Applicant transacts business (e.g. PCI standards)?	<input type="checkbox"/> Yes <input type="checkbox"/> No
Does the Applicant have and enforce policies concerning the encryption of internal and external communication?	<input type="checkbox"/> Yes <input type="checkbox"/> No
Are users able to store data to the hard drive of portable computers or portable media devices such as USB drives?	<input type="checkbox"/> Yes <input type="checkbox"/> No
Does the Applicant encrypt data stored on laptop computers and portable media?	<input type="checkbox"/> Yes <input type="checkbox"/> No
Please describe any additional controls the Applicant has implemented to protect data stored on portable devices:	
What format does the Applicant utilize for backing up and storage of computer system data?	
<input type="checkbox"/> Tape or other media <input type="checkbox"/> Online backup service <input type="checkbox"/> Other:	

Are tapes or other portable media containing backup materials encrypted?	<input type="checkbox"/> Yes <input type="checkbox"/> No
Are tapes or other portable media stored offsite using secured transportation and secured storage facilities?	<input type="checkbox"/> Yes <input type="checkbox"/> No
If stored offsite, are transportation logs maintained?	<input type="checkbox"/> Yes <input type="checkbox"/> No
If stored onsite, please describe physical security controls:	

IV. MEDIA CONTROLS

Please describe the media activities of the Applicant or by others on behalf of the Applicant		
<input type="checkbox"/> Television <input type="checkbox"/> Radio <input type="checkbox"/> Print <input type="checkbox"/> Applicant's Website(s) <input type="checkbox"/> Internet Advertising <input type="checkbox"/> Social Media <input type="checkbox"/> Marketing Materials <input type="checkbox"/> Audio or Video Streaming <input type="checkbox"/> Other (please describe:		
Does the Applicant have a formal review process in place to screen any published or broadcast material (including digital content), for intellectual property and privacy compliance prior to any publication, broadcast, distribution or use?	<input type="checkbox"/> Yes	<input type="checkbox"/> No <input type="checkbox"/> N/A
Are such reviews conducted by, or under the supervision, of a qualified attorney?	<input type="checkbox"/> Yes	<input type="checkbox"/> No <input type="checkbox"/> N/A
Does the Applicant allow user generated content to be displayed on its website(s)?	<input type="checkbox"/> Yes	<input type="checkbox"/> No <input type="checkbox"/> N/A

V. RANSOMWARE

1. How often is phishing training conducted to all staff? When was the last such training completed?		
2. Do you strictly enforce Sender Policy Framework (SPF) on incoming e-mails?	<input type="checkbox"/> Yes	<input type="checkbox"/> No <input type="checkbox"/> N/A
3. Do you pre-screen e-mails for potentially malicious attachments and links?	<input type="checkbox"/> Yes	<input type="checkbox"/> No <input type="checkbox"/> N/A
4. Do you provide a quarantine service to your users?	<input type="checkbox"/> Yes	<input type="checkbox"/> No <input type="checkbox"/> N/A
5. Do you have the capability to automatically detonate and evaluate attachments in a sandbox to determine if malicious prior to delivery to the end-user?	<input type="checkbox"/> Yes	<input type="checkbox"/> No <input type="checkbox"/> N/A
6. Can users run MS Office Macro enabled documents on their system by default?	<input type="checkbox"/> Yes	<input type="checkbox"/> No <input type="checkbox"/> N/A
7. Do you use Office 365 in your organisation?	<input type="checkbox"/> Yes	<input type="checkbox"/> No <input type="checkbox"/> N/A
If Yes: Do you use the o365 Advanced Threat Protection add-on?	<input type="checkbox"/> Yes	<input type="checkbox"/> No <input type="checkbox"/> N/A
8. Do you use an endpoint protection (EPP) product across your enterprise?	<input type="checkbox"/> Yes	<input type="checkbox"/> No <input type="checkbox"/> N/A
9. Do you use an endpoint detection and response (EDR) product across your enterprise?	<input type="checkbox"/> Yes	<input type="checkbox"/> No <input type="checkbox"/> N/A
10. Do you use an endpoint application isolation and containment technology?	<input type="checkbox"/> Yes	<input type="checkbox"/> No <input type="checkbox"/> N/A
11. Is a hardened baseline configuration materially rolled out across servers, laptops, desktops and managed mobile devices?	<input type="checkbox"/> Yes	<input type="checkbox"/> No <input type="checkbox"/> N/A
12. What % of the enterprise is covered by your scheduled vulnerability scans?		

13. In what time frame do you install critical and high severity patches across your enterprise?		
14. Do you have any end of life or end of support software?	<input type="checkbox"/> Yes	<input type="checkbox"/> No <input type="checkbox"/> N/A
If Yes: is it segregated from the rest of the network?	<input type="checkbox"/> Yes	<input type="checkbox"/> No <input type="checkbox"/> N/A
15. Have you configured host-based and network firewalls to disallow inbound connections by default?	<input type="checkbox"/> Yes	<input type="checkbox"/> No <input type="checkbox"/> N/A
16. Can your users access e-mail through a web app on a non-corporate device?	<input type="checkbox"/> Yes	<input type="checkbox"/> No <input type="checkbox"/> N/A
If Yes: do you enforce Multi-Factor Authentication (MFA)?	<input type="checkbox"/> Yes	<input type="checkbox"/> No <input type="checkbox"/> N/A
17. Do you use MFA to protect privileged user accounts?	<input type="checkbox"/> Yes	<input type="checkbox"/> No <input type="checkbox"/> N/A
18. Do you manage privileged accounts using tooling?	<input type="checkbox"/> Yes	<input type="checkbox"/> No <input type="checkbox"/> N/A
19. Do your users have local admin rights on their laptop / desktop?	<input type="checkbox"/> Yes	<input type="checkbox"/> No <input type="checkbox"/> N/A
20. Do you provide your users with a password manager software?	<input type="checkbox"/> Yes	<input type="checkbox"/> No <input type="checkbox"/> N/A
21. Do you use a protective DNS service?	<input type="checkbox"/> Yes	<input type="checkbox"/> No <input type="checkbox"/> N/A
22. Do you have a security operations center established?	<input type="checkbox"/> Yes	<input type="checkbox"/> No <input type="checkbox"/> N/A
If Yes: is it in-house or outsourced?	<input type="checkbox"/> In-House	<input type="checkbox"/> Outsourced
23. Are your backups encrypted?	<input type="checkbox"/> Yes	<input type="checkbox"/> No <input type="checkbox"/> N/A
24. Have you tested the successful restoration and recovery of key server configurations and data from backups in the last 6 months?	<input type="checkbox"/> Yes	<input type="checkbox"/> No <input type="checkbox"/> N/A
If Yes, please detail:		
25. Are your backups kept separate from your network ('offline'), or in a cloud service designed for this purpose?	<input type="checkbox"/> Yes	<input type="checkbox"/> No <input type="checkbox"/> N/A
26. Do you use a Cloud syncing service for backups?	<input type="checkbox"/> Yes	<input type="checkbox"/> No <input type="checkbox"/> N/A
If Yes, please detail:		
27. Are you able to test the integrity of back-ups prior to restoration to be confident it is free from malware?	<input type="checkbox"/> Yes	<input type="checkbox"/> No <input type="checkbox"/> N/A
Please describe any additional steps your organization takes to detect and prevent ransomware attacks:		

VI. PRIOR CLAIMS AND CIRCUMSTANCES

Does the Applicant or other proposed insured (including any director, officer or employee) have knowledge of or information regarding any fact, circumstance, situation, event or transaction which may give rise to a claim, loss or obligation to provide breach notification under the proposed insurance?	<input type="checkbox"/> Yes <input type="checkbox"/> No
If Yes, please provide details:	

During the past 5 years has the Applicant:	
Received any claims or complaints with respect to privacy, breach of information or network security, unauthorized disclosure of information, or defamation or content infringement?	<input type="checkbox"/> Yes <input type="checkbox"/> No
Been subject to any government action, investigation or subpoena regarding any alleged violation of a privacy law or regulation?	<input type="checkbox"/> Yes <input type="checkbox"/> No
Notified consumers or any other third party of a data breach incident involving the Applicant?	<input type="checkbox"/> Yes <input type="checkbox"/> No
Experienced an actual or attempted extortion demand with respect to its computer systems?	<input type="checkbox"/> Yes <input type="checkbox"/> No
If Yes, please provide details of any such action, notification, investigation or subpoena:	

VII. SIGNATURE

THE UNDERSIGNED IS AUTHORIZED BY THE APPLICANT TO SIGN THIS REQUEST FORM ON THE APPLICANT'S BEHALF AND DECLARES THAT THE STATEMENTS CONTAINED IN THE INFORMATION AND MATERIALS PROVIDED TO THE INSURER IN CONNECTION WITH THIS REQUEST FORM AND THE UNDERWRITING OF THIS INSURANCE ARE TRUE, ACCURATE AND NOT MISLEADING. SIGNING OF THIS REQUEST FORM DOES NOT BIND THE APPLICANT OR THE INSURER TO COMPLETE THE INSURANCE, BUT IT IS AGREED THAT THE STATEMENTS CONTAINED IN THIS REQUEST FORM AND ANY OTHER INFORMATION AND MATERIALS SUBMITTED TO THE INSURER IN CONNECTION WITH THE UNDERWRITING OF THIS INSURANCE ARE THE BASIS OF THE CONTRACT SHOULD A POLICY BE ISSUED, AND HAVE BEEN RELIED UPON BY THE INSURER IN ISSUING ANY POLICY.

THIS REQUEST FORM AND ALL INFORMATION AND MATERIALS SUBMITTED WITH IT SHALL BE RETAINED ON FILE WITH THE INSURER AND SHALL BE DEEMED ATTACHED TO AND BECOME PART OF THE POLICY IF ISSUED. THE INSURER IS AUTHORIZED TO MAKE ANY INVESTIGATION AND INQUIRY AS IT DEEMS NECESSARY REGARDING THE INFORMATION AND MATERIALS PROVIDED TO THE INSURER IN CONNECTION WITH THE UNDERWRITING AND ISSUANCE OF THE POLICY.

THE APPLICANT AGREES THAT IF THE INFORMATION PROVIDED IN THIS REQUEST FORM OR IN CONNECTION WITH THE UNDERWRITING OF THE POLICY CHANGES BETWEEN THE DATE OF THIS REQUEST FORM AND THE EFFECTIVE DATE OF THE INSURANCE, THE APPLICANT WILL, IN ORDER FOR THE INFORMATION TO BE ACCURATE ON THE EFFECTIVE DATE OF THE INSURANCE, IMMEDIATELY NOTIFY THE INSURER OF SUCH CHANGES, AND THE INSURER MAY WITHDRAW OR MODIFY ANY OUTSTANDING QUOTATIONS OR AUTHORIZATIONS OR AGREEMENTS TO BIND THE INSURANCE.

I HAVE READ THE FOREGOING REQUEST FORM FOR INSURANCE AND REPRESENT THAT THE RESPONSES PROVIDED ON BEHALF OF THE APPLICANT ARE TRUE AND CORRECT.

Signed: _____ Date: _____

Print Name: _____ Title: _____