Beazley Cyber Application

Basic Information			
Company Name:			
Business Description:			
Registered Address:			
Email Address*			
Financial Information	***Most recent period***	***Prior accounting period***	***Next 12 months***
Total Revenue:	$	$	$

*By providing an email address, you are giving consent to be onboarded to our information portal available to all Beazley policy holders. The portal offers insights to how Beazley supports your business, as well as current trends and topics regarding information security.

**Please Note: We understand that it is not always as simple as a yes or no answer, and encourage the use of our commentary section or a separate document to further explain any answers you feel are not satisfied by the form options below. In addition, we ask you to offer any additional comments regarding other measures you may have in place that you feel are relevant to supporting this application. Thank you.

1.	Network Governance	
1.1	Do you have a named individual in charge of information security (e.g. CISO) that reports into the Board/CEO?	☐Yes (Internal) ☐Yes (External) ☐ No
1.2	Does a documented baseline security framework exist across all operations, entities, subsidiaries including international locations? Is this subject to annual review to ensure best practices are updated?	☐ Yes ☐ No If partial, please explain
1.3	Does a documented asset inventory exist, which categorises all systems, softwares and data by level of sensitivity or criticality?	☐ Yes ☐ No
	If yes: Has this document been assessed in the past 12months to ensure its validity?	☐ Yes ☐ No
1.4	In the past 12months, has the client had an audit/review conducted across all locations to ensure compliance is being met with their own internal standards?	☐ Internal ☐ Third Party ☐ None
	If yes to the above, have all remedial items been formally approved for implementation?	☐ Sign off approved ☐ Implementations complete ☐ N/A
1.5	Do you require all third parties pursuant to a written contract, whom provide hosting, processing or other IT services to the business to be compliant with security framework standards?	☐Yes ☐ No Choose an item.
	If yes: Do you require confirmation on an annual basis that vendors still meet these standards?	☐Yes ☐ No
1.6	What percentage of the IT budget do you dedicate to security?	Details:
1.7	Do you have an incident response plan which addresses network incidents and data breaches?	Have a plan : ☐Yes ☐ No Tested in last year : ☐Yes ☐ No

2.	Information Security	
2.1	With respect to how many unique individuals do you store, process or otherwise interact with personal data (information from which an individual may be identified)?	Choose an item.
2.2	Is personal data encrypted? In transit At rest	☐Yes ☐ No ☐Yes ☐ No

2.3	Do you implement tighter security measures for sensitive personal data (records of ethnicity, religion, sexual preferences or medical conditions)?	☐Yes ☐ No
2.4	How many payment card transactions do you process (if applicable) ?	Choose an item.
2.5	Do you store any payment card information?	☐Yes ☐ No
2.6	If the answer to 2.5 is yes, do you comply with PCI-DSS?	☐Yes ☐ No
2.7	If the answer to 2.5 is no, does your vendor comply?	☐Yes ☐ No
3.	**Ransomware Protection**	
3.1	Do you pre-screen emails for potentially malicious attachments and links?	☐Yes ☐ No
3.2	Do you provide a quarantine service to your users?	☐Yes ☐ No
3.3	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?	☐Yes ☐ No
3.4	Do you strictly enforce Sender Policy Framework (SPF) on incoming e-mails?	☐Yes ☐ No
3.5	How often is phishing training conducted to all staff?	Choose an item.
3.6	Can your users access email through a web app on a non-corporate device?	☐Yes ☐ No
	If yes: do you enforce Multi-Factor Authentication (MFA)?	☐Yes ☐ No
3.7	Do you use Office 365 in your Organisation?	☐Yes ☐ No
	If yes: Do you use the O365 Advance Threat Protection add-on, or similar alternative product?	☐Yes ☐ No
3.8	Do you use an endpoint protection (EPP) product across your enterprise?	Choose an item.
3.9	Do you use an Advanced Endpoint Protection and Response (EDR) product across your enterprise?	Choose an item.
3.10	Do you use MFA to protect privileged accounts?	☐Yes ☐ No
3.11	Is a hardened baseline configuration materially rolled out across servers, laptops, desktops, and managed mobile devices?	Choose an item.
3.12	What % of the enterprise is covered by your scheduled vulnerability scans?	
3.13	In what time frame do you install critical and high severity patches across your enterprise once received?	Choose an item.
3.14	Have you configured host-based and network firewalls to disallow inbound connections by default?	Choose an item.
3.15	Do you use a protective DNS service (E.g Quad9, OpenDNS or PDNS)?	☐Yes ☐ No
3.16	Do you use an endpoint application isolation and containment technology?	Choose an item.
3.17	Do your users have local admin rights on their laptop/desktop?	☐Yes ☐ No
3.18	Can users run MS Office Macro enabled documents on their system by default?	☐Yes ☐ No
3.19	Do you provide your users with a password manager software?	☐Yes ☐ No
3.20	Do you manage privileged accounts using tooling? E.g CyberArk	Choose an item.
3.21	Do you have a security operations center established? Either in-house or outsourced	Choose an item.
3.22	Are your backups encrypted?	☐Yes ☐ No
3.23	Are your backups kept separate from your network (offline), or in a cloud service designed for this purpose?	Choose an item.

3.24	Do you use a cloud syncing service (e.g Dropbox, OneDrive, Sharepoint, Google Drive) for back ups?	☐Yes ☐ No
3.25	How regularly do you back up data to the offline/cloud environment?	Choose an item.
3.26	Is access to backups, whether on prem, or in the cloud, limited to unique administrative not used for any other function?	☐Yes ☐ No
3.27	Is access to backups, whether on prem or in the cloud, authenticated via MFA?	☐Yes ☐ No
3.28	Have you tested the successful restoration and recovery of key server configurations and data from back ups in the last 6months?	Choose an item.
	Have you investigated, and put in place, necessary bandwidth to download large amounts of data from Cloud back ups quickly?	Choose an item.
3.29	Are you able to test the integrity of back ups prior to restoration to be confident it is free from malware?	Choose an item.
4. Business Interruption		
4.1	Do you have a fall-back for all mission-critical or revenue-generating processes?	☐Yes (Alternate) ☐Yes (Manual) ☐ No
4.2	If you rely on third party hosting to conduct mission-critical or revenue-generating parts of your business, do you have an alternative solution in the event of a provider failure?	☐Yes ☐ No
4.3	Do you have fault-tolerant architecture for mission-critical or revenue-generating equipment?	☐Yes ☐ No
4.4	Do you enforce mitigating controls for all end of life systems? Please tick all which apply:	☐ Segregation/DMZ ☐ No internet connection ☐ Outbound connection only ☐ If other, please offer comments
4.5	Do you segregate your Operational/Mission Critical technology from the wider user/internet facing environment (Emails etc)?	☐Yes ☐ No
4.6	What controls do you have in place for SCADA/DCS? Please tick all which apply	☐ICS-specific risk management ☐Network Segmentation ☐Air Gapping ☐Boundary Protection ☐Redundancy
4.7	Do you segregate your network by geography, to isolate any potential malware infections?	Yes ☐ No, flat network exists across the company ☐
4.8	In the event of an outage to your operational technology, how long could the business sustain orders with current inventory levels?	Choose an item. If other, please offer comments
4.9	If you rely on Third Party hosting for any mission critical services/data stores, what high availability/redundancy provisions do they provide? Please tick all which apply:	☐ Geographic Redundancy ☐ Redundant Infrastructure ☐ Failover capabilities/Cluster ☐ If other, please offer comments
4.10	Do you have alternative providers for mission critical services to add resilience in the event of a provider failure	☐Yes ☐ No
4.11	Do you build excess capacity into your production process, to allow other plants to	☐Yes ☐ No

	increase production in the event of an isolated facility failure?	Please offer comments if required
5.	**Electronic Crime (if applicable)**	
5.1	Do you accept funds transfer instructions from clients over the telephone, email, text message or similar method of communication? If YES, prior to complying with the instruction do you authenticate such instructions by: a. Calling the customer at a predetermined number? b. Sending a text message to a predetermined number? c. Requiring receipt of a code known only to the customer to confirm identity? d. Some other method or combination of the above? Please describe.	NA, we do not accept funds via these modes of communication☐ A ☐ B ☐ C ☐ D ☐
5.2	Do you confirm all changes to vendor/supplier details (including routing numbers, account numbers, telephone numbers and contact information) by a direct call using only the contact number previously provided by the vendor/supplier before the request was received?	☐Yes ☐ NO
5.3	Do you verify all vendor/supplier bank accounts by a direct call to the receiving bank, prior to being established in the accounts payable system?	☐Yes ☐ NO
5.4	Are all employees that are responsible for wire transfer provided anti-fraud training, including but not limited to detection of social engineering, phishing and other scams?	☐Yes ☐ No
6.	**Prior Claims & Circumstances**	
6.1	Does the applicant or other proposed insured (or any director, officer or employee of the applicant or other proposed insured) have knowledge of or information regarding any fact, circumstance, situation, event or transaction which may give rise to a claim or loss or obligation to provide breach notification under the proposed insurance?	☐Yes ☐ No Detail:
6.2	During the past 5 years has the applicant had any cyber related incidents or claims?	☐Yes ☐ No Detail:

7. Warranty Statement

The Applicant warrants that all representations made material to the risk are true and verify to the best of their knowledge upon reasonable enquiry, that all information contained herein is accurate.

The Applicant declares that no member of the **Control Group**, as defined within the policy wording, is aware of any acts, errors, omissions, circumstances or incidents that are likely to give rise to a claim or loss under the proposed insurance.

By: Date: / /

Must be signed and dated by member of the Control Group, as defined within the policy: **Control Group** means any principal, partner, corporate officer, director, Member, general counsel (or most senior legal counsel) or risk manager of the **Insured Organisation**; and any individual in a substantially similar position.

**Aditional Commentary Section. Please use a separate document if appropriate: