beazley

Cyber Insurance Application

For Applicants with revenues lower than £/€ 250M

NOTICE: THIS POLICY'S LIABILITY INSURING AGREEMENTS PROVIDE COVERAGE ON A CLAIMS MADE AND REPORTED BASIS AND APPLY ONLY TO CLAIMS FIRST MADE AGAINST THE INSURED DURING THE POLICY PERIOD OR THE OPTIONAL EXTENSION PERIOD (IF APPLICABLE) AND REPORTED TO THE UNDERWRITERS IN ACCORDANCE WITH THE TERMS OF THIS POLICY. AMOUNTS INCURRED AS CLAIMS EXPENSES UNDER THIS POLICY WILL REDUCE AND MAY EXHAUST THE LIMIT OF LIABILITY AND ARE SUBJECT TO RETENTIONS.

PLEASE READ THIS POLICY CAREFULLY.

Responses to this application should be accurate as of the date that the application is signed and dated below. Please provide responses below concerning the Information Technology (IT) environment of your organization and any subsidiaries for which the insurance is being sought. You may use the space under the heading "Additional Disclosures & Clarifications" to clarify any answers that may be incomplete or require additional detail.

General Information

Full name _____

Headquarters address _____

Business description _____

Industry classification _____

Website URLS(s) _____

Number of employees _____

1. Total revenue:

	Most recent fiscal year	Current fiscal year (projected)
GBP	_____	_____

2. Do you have any revenue-generating operations outside your domiciled country? ☐ No ☐ Yes, percentage ____ %

3. Cybersecurity point of contact (CISO/Risk Manager or equivalent role):

First Name	Last Name	Job Title	Email	Telephone
_____	_____	_____	_____	_____

beazley

4. Are you engaged in any of the following business activities?

   - Adult content, gambling or cannabis (containing THC) as a grower, wholesaler or medical/recreational retailer;
   - Cryptocurrency, blockchain technology, payment processing or debt collection;
   - Data processing/aggregation, storage or hosting services to third parties as a professional service (e.g., as a managed services provider (MSP) or data aggregator); or
   - Managed care or accountable care.

   ☐ No ☐ Yes

Cybersecurity Controls

5. Do you require Multi-Factor Authentication (MFA) for remote access to your network (both cloud-hosted and on-premises, including via Virtual Private Networks (VPNs))?

   ☐ No ☐ Yes ☐ Remote access not permitted

6. Do you require MFA for access to web-based email?

   ☐ No ☐ Yes ☐ Access not permitted/no web-based email

7. What security controls do you have in place for incoming email? Choose all that apply.

   ☐ Screening for malicious attachments ☐ Screening for malicious links ☐ Tagging external emails

8. How often do you conduct interactive social engineering (i.e., phishing) training?

   ☐ Never/not regularly ☐ Annually ☐ ≥2x per year

9. Do you protect all company devices with anti-virus, anti-malware, and/or endpoint protection software?

   ☐ No ☐ Yes

10. Do you regularly back up your business critical data?

    ☐ No ☐ At least monthly ☐ At least weekly or daily

11. Do you, or an outsourced service provider on your behalf, actively manage and install critical patches across your internet-facing systems?

    ☐ No ☐ Yes

Additional Cybersecurity Controls (only for Applicants with revenues greater than $35M)

12. Do you use the Microsoft 365 Defender add-on or an equivalent cybersecurity product with advanced threat hunting to protect against phishing and business email compromise? ☐ No ☐ Yes

13. Do you disable macros in your office productivity software by default? (E.g., Microsoft Office, Google Workspace) ☐ No ☐ Yes

beazley

14. What security solutions do you use to prevent or detect malicious activity on your network?

Security solution	Vendor
a. Endpoint Protection Platform (EPP)	
b. Endpoint Detection and Response (EDR)	
c. Managed Detection and Response (MDR)	

15. Do you use a hardened baseline configuration across all (or substantially all) of your devices? ☐ No ☐ Yes

16. If you rely on a cloud-based backup service, is it a "syncing service"? (E.g., DropBox, OneDrive, SharePoint, Google Drive) ☐ No ☐ Yes ☐ No cloud backups

17. Do you have an incident response plan for network intrusions and malware incidents? ☐ No ☐ Yes

Media Controls

18. a. Do you 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? ☐ No ☐ Yes

    b. If "Yes" to a., are such reviews conducted by, or under the supervision of, an attorney? ☐ No ☐ Yes

19. Do you have notice and take-down procedures in place to address potentially libelous, infringing, or illegal content on your website(s) (e.g., DMCA or similar)? ☐ No ☐ Yes

Money Transfer Controls

20. Are employees who are responsible for disbursing or transmitting funds provided anti-fraud training, including detection of social engineering, phishing, business email compromise and other scams, on at least an annual basis? ☐ No ☐ Yes

21. When a vendor or supplier requests any change to its account details (including routing numbers and account numbers), do you confirm requested changes via an out-of-band authentication (a method other than the original means of request)? For example, if a request is made by email, a follow-up phone call is placed to confirm that the supplier or vendor made the request. ☐ No ☐ Yes

Mergers & Acquisitions

22. Have you, within the past 12 months, completed or agreed to a merger, acquisition, or consolidation? ☐ No ☐ Yes

    If "Yes", please provide details:

beazley

Prior Claims & Circumstances

23. Do you or any other proposed insured (including any director, officer, or employee) have knowledge of or information regarding any fact, circumstance, situation, event, or transaction that may give rise to a claim, loss, or obligation to provide breach notification under the proposed insurance? ☐ No ☐ Yes

24. During the past five years, have you:

    a. Received any claims or complaints with respect to privacy, breach of information, breach of network security or unauthorized disclosure of information? ☐ No ☐ Yes

    b. Been subject to any government action, investigation or subpoena regarding any alleged violation of a privacy law or regulation? ☐ No ☐ Yes

    c. Notified customers or any other third party of a data breach incident? ☐ No ☐ Yes

    d. Experienced an actual or attempted extortion demand (including ransomware) with respect to your computer systems? ☐ No ☐ Yes

    e. If you answered "Yes" to any of a., b., c., or d., above, have you experienced three or more events described above, and/or did you incur a single event loss or total of all losses of more than $25,000, and/or is an insurance claim still open in connection with any of the events described above? (If you answered "No" to a., b., c., and d., please leave this question blank) ☐ No ☐ Yes

If you answered "Yes" to question 23 or any parts of question 24, please provide details regarding all such facts, circumstances, situations, incidents, or events in the "Additional Disclosures & Clarifications" section, below.

Additional Disclosures & Clarifications

Please use the space below to clarify any answers above that may be incomplete or require additional detail.

Signature Section

Before this insurance contract is entered into, the proposer must make a fair presentation of the risk in accordance with Section 3 of the Insurance Act 2015. If you are unsure about what is required to meet your duty of fair presentation then please contact your broker for further information.

On behalf of the proposer, you confirm that all the answers provided in this application together with any oral or written statement provided to us are true, complete and not misleading. On behalf of the proposer, you agree that you will inform us of any material changes to the information supplied in this application prior to the inception of any insurance policy. If there are any material changes prior to inception then we may withdraw or modify any terms accordingly. We will not provide any indemnity in respect of such liability from such material change unless we have agreed in writing to accept the altered risk.

beazley

I/we declare that I/we have made a fair presentation of the risk, by disclosing all material matters which I/we know or ought to know or, failing that, by giving the Insurer sufficient information to put a prudent insurer on notice that it needs to make further enquiries in order to reveal material circumstances.

This declaration and application is signed by a director or officer of the proposer who is responsible for arranging insurance on behalf of the proposer.

This Proposal Form should be signed no earlier than 30 days prior to inception of the policy.

For digital signature, click the red tab to create a digital ID or import an existing digital ID:

Print Name: _____

Job Title: _____ Company: _____

Signed: _____ Date: _____