beazley

Cyber Insurance Application £/€ 250M+

For Applicants with revenues greater 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
_____	_____	_____	_____	_____

4. Are significant changes in the nature or size of your business anticipated in the next 12 months? ☐ No ☐ Yes

beazley

5. 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

Records

6. How many individual records do you hold for each type of information? If a record could fall into more than one category, count it toward the most appropriate category.

   a. Payment Card Information (PCI) _____

   b. Protected Health Information (PHI) _____

   c. Biometric Information _____

   d. Personally Identifiable Information (PII) _____

Cybersecurity Controls

7. 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

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

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

9. What security controls do you have in place to protect Domain Administrator accounts?

   a. Do you enforce MFA for privileged accounts in Azure Active Directory (AAD) (including the members of the AAD Domain Controller administrators group)?

      ☐ No ☐ Yes ☐ We do not use AAD

   b. Are Domain Administrators permitted to connect only to domain controllers (and <u>not</u> email or connect to the internet)?

      ☐ No ☐ Yes

   c. Are Domain Administrators configured with unique, random, and long (>25 characters) passwords?

      ☐ No ☐ Yes

beazley

10. 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

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

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

12. Do you regularly backup your business critical data?

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

13. Where do you backup your business critical data? Choose all that apply.

☐ Corporate network ☐ Cloud service ☐ Offline

14. If you rely on a cloud-based backup service, is it a "syncing service"? (E.g., DropBox, OneDrive, Google Drive)

☐ No ☐ Yes ☐ No cloud backups

15. How frequently do you perform a test restoration from backups?

☐ Never/not regularly ☐ Annually ☐ 2-3 times per year ☐ Quarterly or more often

16. 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)	

17. Do you have a Security Operations Center (SOC)?

☐ No ☐ Yes, working hours only ☐ Yes, 24/7

18. a. Do you have any end-of-life or end-of-support software on your network?

☐ No ☐ Don't know ☐ Yes

b. If "Yes" to a., is the software segregated on your network?

☐ No ☐ Some is, some isn't ☐ Yes

19. Are network firewalls configured to disallow inbound connections by default? ☐ No ☐ Yes

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

21. Do you permit ordinary users local administrator rights to their devices (e.g., laptops)? ☐ No ☐ Yes

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

beazley

23. Do you, or an outsourced service provider on your behalf, actively manage and install critical patches across your internet-facing systems? ☐ No ☐ Yes

24. 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

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

26. Do you use any remote desktop clients (e.g., Microsoft Remote Desktop, TeamViewer, Virtual Network Computing (VNC), AnyDesk) that are exposed directly to the internet? ☐ No ☐ Yes

PCI Controls

27. a. Do you accept payment cards for goods sold or services rendered? ☐ No ☐ Yes

    b. If "Yes" to a., do you ensure point-to-point encryption of payment card data? ☐ No ☐ Yes

    c. If "Yes" to a., do you maintain payment card data on your network?

    ☐ No ☐ Yes, unencrypted ☐ Yes, tokenized or encrypted

Media Controls

28. 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

29. 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

30. 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

31. 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

beazley

Operational Technology Controls

Complete this section *only if* (1) you are in the manufacturing, construction, transportation, warehousing, utilities, and wholesale trade industries; (2) you have Operational Technology (OT) in your environment; *and* (3) your OT is accessible (i.e., not air-gapped) from your IT network or the internet.

☐ Check here if these questions do not apply to you based on the above criteria.

32. Is your OT environment segmented from your Information Technology (IT) environment(s)? ☐ No ☐ Yes

33. Is your OT environment segmented from the internet? ☐ No ☐ Yes

34. Do you enforce MFA for employee remote access to your OT environment? ☐ No ☐ Yes ☐ Not permitted

35. Do you enforce MFA for third-party remote access to your OT environment? ☐ No ☐ Yes ☐ Not permitted

Mergers & Acquisitions

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

    If "Yes", please provide details:

Prior Claims & Circumstances

37. 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

38. 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

If you answered "Yes" to question 37 or any parts of question 38, please provide details regarding all such facts, circumstances, situations, incidents, or events in the "Additional Disclosures & Clarifications" section, below.

beazley

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.

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: _____