Logo

Description automatically generated

Cyber Application ($50M - $100M Revenue)

**General Information**

**Applicant:**

**Address:**

**Subsidiaries to be covered under the proposed Policy:**

**Operating Countries:**

**Insured Name:**

**Insured Email:**

**Website:**

**Revenues of the last compete Financial Year:**

1. Are all computers in your organisation running Windows 10 or later? Select
2. Do you protect all of your devices with anti-virus, anti-malware, and/or endpoint protection software? Select
3. Do you install all security patches (e.g. those issued by Microsoft) within 30 days of release? Select
4. Do you use cloud-based email services (e.g. Office365, Gmail, Microsoft Outlook on the web)? Select
   1. **If Yes**, have you enabled multifactor authentication (MFA) on all accounts? Select
5. Do you scan all incoming emails for malicious attachments and/or links? Select
6. Do you allow remote access to your network (e.g. enabling employees to work from home)? Select

**If Yes:**

* 1. Do you require multi-factor authentication (MFA) for all remote connections? Select
  2. Do you use a virtual private network (VPN) for all remote connections? Select

1. Have you taken measures to ensure that you comply with all privacy and data protection laws and regulations that apply to your organisation (e.g. PCI, CCPA, HIPAA, GDPR)? Select
2. Are firewalls installed at all gateways and configured to block inbound connections by default? Select
3. Are access controls employed using the principle of least privilege? Select
4. Do you maintain physically disconnected ‘offline’ back-ups (e.g. tape drives) for all critical data? Select
5. Have you tested the successful restoration and recovery of key server configurations and data from backups in the last 6 months? Select
6. Have you disabled all Remote Desktop Protocol (RDP) ports? Select
7. Do you encrypt all personal and confidential data in-transit and when stored on portable devices? Select
8. Have you taken measures to ensure that your organisation’s website and print content do not infringe on any trademarks or copyrights? Select
9. Do you utilise next generation anti-virus or behavioural analysis software, including Endpoint Detection and Response (EDR) tools? Select
   1. **If Yes**, please state which tools are used (e.g CrowdStrike Falcon, SentinelOne)?
10. Are employees trained in phishing and social engineering techniques? Select
11. Do you utilise email filtering tools and/or software? Select
    1. **If Yes**, please state which software and/or tools are used (e.g. Proofpoint with e.g. SPF. DKIM and DMARC enabled
12. Have you disabled all local administrator accounts on workstations and servers? Select
    1. **If No**, do all local administrator accounts utilise a unique password? Select
13. Do you run any version of Windows Server? Select

**If Yes**,

* 1. Do you take frequent back-ups of Active Directory servers? Select
  2. Do all login attempts to Domain Administrator accounts require multifactor authentication (MFA)? Select

*Please add any additional commentary/clarifications to answers provided here:*

**Historical Information**

**In the past 5 years have you or entity falling within the definition of ‘Insured’ under the proposed Policy:**

* Received a claim or complaint regarding privacy, data protection or network security? Select
* Been subject to any government or regulatory investigation regarding an alleged violation of privacy and/or data protection legislation/regulation? Select
* Received a complaint or cease and desist demand alleging intellectual property infringement? Select
* Notified any persons of a privacy violation and/or data breach incident? Select
* Received an extortion demand relating to your data and/or computer systems? Select
* Experienced a network outage that resulted in a significant disruption to your operations? Select

*If you have answered “Yes” to any of the above, please provide details, including cause of loss; financial costs incurred to date; and remediation action taken to prevent recurrence of incident:*

|  |  |  |
| --- | --- | --- |
| **Date of Incident** | **Expected Financial Costs Incurred** | **Description of Incident & Remediation Performed** |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |

**Representation on Behalf of Your Entire Organisation**

Please confirm that the answers provided to the questions in this application are applicable to your entire organisation, including all subsidiaries for whom you are seeking cover under the proposed cyber insurance policy. Select

If the answers provided to the questions in this application are **not** applicable to your entire organisation, please outline where any exceptions/inconsistences exist:     

*I declare that after proper enquiry the statements and particulars given above are true and that I have not mis-stated or suppressed any material fact.*

*I agree that this proposal form, together with any other material information supplied by me shall form the basis of any contract of insurance effected thereon.*

*I undertake to inform underwriters of any material alteration to these facts occurring before the completion of the contract.*

***Signature:***

***Title:***

***Date:***